Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ)
ISSUE (35), August (2020)

ISSN: 2616-9185

Mechanisms for activating the protection and prevention of cybercrime
(Creating a seizure for cybercrime)

Dr. Nibras salim khudhair

Law department, Al kunooze University College

Contact. Nibras salim nibras.s@kunoozu.edu.iq

Abstract

In many countries, jurisdiction for investigation and adjudication of cybercrime returns to the seizure device in charge of research and investigation, as well as to the ordinary judiciary in its penal aspect, which makes the detection and proof of this type of crime very difficult, the lack of experience in the field of computers, the Internet and electronic transactions, and on the other hand, there are fraudulent hackers who have high skills and keep pace with everything new in the world of informatics and communication. Therefore it was necessary to call for the creating a seizure, a special system or entity to investigate this type of crime, which does not depend on physical strength and raining as much as it relies on technical skill in the field of information and communication technology, as a first stage to create a judicial entity to rule on these crimes.

Keywords

Mechanisms, protection, prevention, cybercrime, seizure

Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ)
ISSUE (35), August (2020)

ISSN: 2616-9185

ملخص البحث

في العديد من البلدان ، يعود الاختصاص القضائي للتحقيق والفصل في الجرائم السيبرانية إلى جهاز الحجز المسؤول عن البحث والتحقيق ، وكذلك إلى القضاء العادي في جانبه الجنائي ، مما يجعل الكشف عن هذا النوع من الجرائم وإثباته صعبًا للغاية ، قلة الخبرة في مجال الحاسب الآلي والإنترنت والمعاملات الإلكترونية ، ومن ناحية أخرى ، هناك قراصنة مخادعون لديهم مهارات عالية ومواكبة كل ما هو جديد في عالم المعلوماتية والاتصالات. لذلك كان من الضروري الدعوة إلى إنشاء ضبط أو نظام خاص أو كيان للتحقيق في هذا النوع من الجرائم ، والذي لا يعتمد على القوة البدنية والأمطار بقدر ما يعتمد على المهارات التقنية في مجال تكنولوجيا المعلومات والاتصالات ، كمرحلة أولى لإنشاء كيان قضائي للبت في هذه الجرائم.

تعد الجريدة الإلكترونية من أكثر المواضيع انتشارا على المستوى الدولي والإقليمي والمحلي. وقد اكتسبت هذه الجريمة ، نتيجة الاستخدام السلبي للتكنولوجيا والتكنولوجيات ذات الصلة ، جزءًا كبيرًا من الاهتمام في هذا الجانب ، نظرًا لحجم الآثار الناشئة عن هذه الظاهرة الحديثة إلى حد ما وفي جميع مجالات الحياة.

يواجه المشرع جرائم مختلفة مع التجريم والعقاب كشكل من أشكال الرقابة الموضوعية. من أجل السيطرة على هذه الجريمة والقبض على مرتكبها ، يوفر المشرع القدرات البشرية والمادية لذلك كشكل من أشكال الرقابة الإجرائية ، وتبقى المسألة هنا طبيعية لا تثير أي مشكلة طالما نحن فيما يتعلق بالتقليدية العادية الجرائم ، لكنه يختلف إذا كنا نتعامل مع جرائم غير عادية ، جرائم في عالم افتراضي.

الكلمات الافتتاحية

الآليات والحماية والوقاية والجرائم الإلكترونية والنوبات.

1. Introduction

The electronic newspaper is one of the most prevalent topics at the international, regional and local levels. This crime, as a result of the negative use of technology and related technologies, has taken a large part of attention in this aspect, due to the magnitude of the effects arising from this somewhat recent phenomenon and in all areas of life.

The legislator faces various crimes with criminalization and punishment as a form of substantive control. In order to control this crime and arrest its perpetrator, the legislator provides the human and material capabilities for that as a form of procedural control, and the matter here remains normal that does not raise any problem as long as we are in relation to ordinary traditional crimes, but it differs if we are dealing with extraordinary crimes, crimes in a world hypothetical.

ISSN: 2616-9185

Cybercrime is any unlawful behavior that interferes with electronic operations or compromises the security of information devices and the data that addresses them. These crimes altered the balance of the investigation, so it is no longer related to physical strength or combat skills, but to the extent of the investigator's technical knowledge and proficiency of the requirements of automated media and communication, this knowledge is what contributes to the arrest of the cybercriminal.

Objectives of the study

In light of the increase in Cybercrime and the diversity of their patterns and methods, the specialized agencies in research and investigation, headed by the judicial seizure, were unable to keep pace with this development and pursue this type of crime, which prompted many countries to create specialized agencies that can deal with this type of crime.

Study Problem

Hence the problem that this paper attempts to answer is if the Arab have legislation provided human and material capabilities for research and investigation in cybercrime, and We will try to answer this problem according to the following two topics: The first topic: motives for creating a seizure specialized with cyber-crime, and The second topic: models for cybercrime devices "Internet police".

2. motives for creating a seizure specialized with cyber-crime

Cybercrime is a modern day crime and its duration is no less than the most serious crime. This is in view of the severe damage that this type of crime can cause, hence the voices calling for the necessity of fighting cybercrime, due to the characteristics that distinguish it from the rest of the ordinary crimes.

2.1. the modernity of cybercrime on judicial seizure devices

Members of the judicial police are used to researching and investigating ordinary crimes that take place in the physical real.

ISSN: 2616-9185

Where it is easy to navigate to the place of the crime, search for evidence and infer the perpetrators of the crimes, arrest them and investigate them, which is a process that requires readiness and essential physical skill, until cybercrime appeared and it is completely different from traditional crimes in terms of how they occur and their effects and the methods used to commit it, it created an emergency in the judicial investigation and investigation devices, and then the voices were raised to create special devices for research and investigation in such crimes, which do not depend on physical and physiological training but rather depends on a certain practical and intellectual level and special skills in the field of communication and the Internet. So that the investigator can investigate and infer in the virtual world and chase criminals in the electronic environment (Hisham, Farid, 2000, p.45), which is what the Budapest Cultural Authority referred to with information criminality, which called for the necessity of creating such devices at the national level and the necessary legislative procedures for that, as stated in its article (١٤) that: "Each party must adopt legislative or other procedures that it deems necessary for the establishment of authorities and the setting of procedures stipulated in this section for the purpose of special criminal techniques or procedures(1)." The agreement allowed each party to reserve the right not to apply the procedures referred to except only for certain crimes (. Hilali, 2007, p. 174) .

Most of the Arab legislation did not provide for the existence of specialized judicial bodies to investigate and adjudicate Cybercrime, and therefore the jurisdiction to consider these cases is due to the ordinary judiciary in its criminal aspect, which makes the separation of such crimes from the difficulty what was due to the lack of knowledge and scientific and technical expertise of judicial men in this field, and although the law allows the judge to seek expertise to determine the circumstances of the case and reach the truth, It is the judge's experience and referral of the facts and data of the case that contribute to revealing the truth.

It is related to seizure members who are not ready in the face of professional criminals, as the competence in research and investigation in cybercrime belongs to the members of the judicial police mentioned in the law, which puts us before an unequal equation related to the research, investigation devices, where their expertise in the field of computer and internet world is lacking And electronic transactions on the one hand, and on the other hand,

they are fraudulent hackers who enjoy high skills and keeping up of everything new in the world of information and communication.

According to the saying that something that is the lost on something does not give it, it is impossible for members of the regular police to search and investigate cybercrimes and deal with their perpetrators. Hence, there is no escape from calling for the existence of specialized devices in this type of crime, Or to work on developing the expertise and skills of the persons in charge of research and investigation, As well as the development of well-studied methods to investigate and prove this type of crime, And taking into account the specificity of the rapid technical development in the field of communication, without neglecting international cooperation in such cases.

2.1.1. Cybercriminal specification

We can extract a set of specifications that characterize the Cybercriminal. And getting to know them helps confront this new pattern of criminals. Professor (parker) is one of the most important researchers who took care of Cybercrime in general and cybercriminal in particular, and parker believes that the Cybercriminal, although it has some special features, but in the end does not go out of being the perpetrator of a criminal act that requires the execution of punishment, and with The following is a presentation of some of the many characteristics of an Cybercriminal, which often distinguishes him from other common criminals: (Younis, Arab, 1994, p.72)

2.1.1.1. the Cybercriminal is a specialized criminal

It has been found in many cases that a number of criminals commit only computer crimes, that is, they specialize in this type of crime, without having anything to do with any other traditional crime. This indicates that a criminal who commits cybercrime is a criminal who mostly specializes in this type of crime.

ISSN: 2616-9185

2.1.1.2. The Cybercriminal is a criminal returning to crime

Many information criminals are due to other computer crimes committed out of a desire to fill the gaps that led to their identification and led to their being brought to trial the previous time. This has led to a return to criminality, and they may well end up next time bringing them to trial

2.1.1.3. the Cybercriminal, a professional criminal

The Cybercriminal enjoys great professionalism in the implementation of his crimes, as he commits these crimes through the computer. It requires a lot of accuracy, specialization and professionalism in this field to reach overcoming the obstacles created by specialists to protect computer systems as in the case of banks and military institutions.

2.1.1.4. the Cybercriminal, a non-violent criminal

A cybercriminal is a criminal who does not resort to violence at all in the implementation of their crimes, because he belongs to a crime - trick - he does not resort to violence in committing his crimes, and this type of crime does not require any degree of effort to do it.

In addition to the above, the Cybercriminal is a smart criminal. And he enjoys social adaptation, that is, he does not hostile to anyone, and he also has the skill and knowledge and in many cases he is highly educated

2.1.2. Cybercriminal characteristics (Francillon, 1997, p. 293)

The Cybercriminal is also distinguished by a set of characteristics that were generally distinguished from other criminals, namely:

2.1.2.1. skill

The implementation of cybercrime requires a degree of skill that the perpetrator possesses, which he may acquire through specialized study in this field, or through experience gained in the field of technology, or merely by social interaction with others, and this is not a rule that the Cybercriminal should be this much Science,

ISSN: 2616-9185

And this is proven by the practical reality that many successful criminals of informatics have not received the skill necessary to commit this type of crime.

2.1.2.2. knowledge

Cyber criminals are distinguished by knowledge, where the Cybercriminal can make a complete picture of his crime, due to the fact that the stage in which cybercrime is practiced, which is the first computer system, the actor can apply his crime to similar systems before the crime is executed

2.1.2.3.The way

It means the capabilities the Cybercriminal needs to complete his crime. Often these ways may be simple and easy to obtain, especially if the system that works with the computer is one of the common systems, but if the system is one of the unfamiliar systems, then these methods are complex and with a degree of difficulty

2.1.2.4. authority

It means the rights and advantages of a cybercriminal that enables him to commit his crime. Many informational criminals have direct or indirect authority to confront the information subject to the crime, and this authority may be represented in the code for entering the system that contains the information and also the authority may be It is the criminal's right to enter the computer and conduct transactions, just as the authority may be legal, it can be illegal, as in the case of stealing the entry code of another person.

2.1.2.5. motivation

It is the desire to achieve material profit in an unlawful manner and is the first motive behind the commission of information crime. Some also see something else, which is that the financial gain is not the motive in most cases to commit information crimes,

but there are many other things that are often the motive, such as revenge on the employer, And also just the desire to conquer the computer system and penetrate its security barrier.

2.2. complex crimes and a crime scene with no limits

2.2.1. Cybercrime is distinct from ordinary crime

One of the most important factors calling for the creating a device specialized in cybercrime, which is the distinct nature of these crimes, as they are crimes that take place in a virtual environment and do not leave material effects, as is the case in ordinary crimes. Among the characteristics and features we also find: Cybercrime is a cross-border crime.

Cybercrime does not recognize geographical borders in a crime that penetrates time and space, as computers and the Internet have an enormous ability to transfer large amounts of information and exchange them between systems separated by thousands of miles in the same time.(Mohamed, 2001, p.94)

The information system does not recognize geographical borders, it is an open society through networks that penetrate time and space without being subject to border guards.

After the emergence of information networks, there are no longer visible or tangible borders that hinder the transmission of information across different countries. The ability of computers and networks to transfer large amounts of information and exchange them between systems separated by thousands of miles has led to a conclusion that multiple places in different countries may be affected by a single information crime at one time. The ease in the movement of information through modern technology systems made it possible to commit a crime through a computer located in a particular country, while the criminal act was achieved in another country. (Al-Momani, 2008, p. 51)

This characteristic of cybercrime, which is that it is a cross-border crime, has created many problems about determining the state with jurisdiction over this crime, as well as about defining the law to be applied in addition to issues related to prosecution procedures, and other points raised by cross-border crimes generally.

ISSN: 2616-9185

The issue known as HIV / AIDS was one of the issues that drew attention to the international dimension of information crime, and the facts of this case that occurred in 1989 are summarized by a person distributing a large number of copies of taking programs that were apparently intended to give some Advice on HIV, but this program in fact contained a virus (Trojan horse) if its operation entails disabling the computer from working, and then a phrase appears on the screen through which the actor requests a sum of money to be sent to a specific address So the victim can get Antivirus. On February 3, 1998, the accused, Joseph Pope, was arrested in Ohio, USA, and she applied from the United Kingdom t to extradite her to stand trial by the English judiciary. Since the transmission of this program took place from within the United Kingdom, and indeed the American judiciary agreed to extradite the accused, and eleven charges of extortion were brought against him, most of which occurred in different countries, but the trial procedures of the accused were not settled due to his mental condition (Sagheer, p. 22), and whatever the matter, this case Its importance in two respects: It is the first time that an accused has been extradited for an information crime , and It is the first time that a person is on trial for preparing a malicious program (virus).

As a result of this special nature of information crime and in view of the seriousness it poses at the international level, and the losses it may cause, extensive international cooperation is required to tackle these crimes, and international cooperation is represented in international treaties and agreements that provide an atmosphere of coordination between member states, which ensures Being cyber criminals and bringing them to a fair trial.

The most important problems related to international cooperation on cybercrime lies in the fact that there is no common concept among countries about the forms of activity that constitutes this crime in addition to the lack of experience of the police and the prosecution and the judiciary in this field to examine the elements of the crime if any and collect evidence about it for conviction in it is an obstacle in front of cooperation in the field of combating this type of crime, therefore, in order to address cybercrime, countries must act in two directions: where different countries legislate appropriate laws to combat these crimes,

And By concluding international agreements, so that criminals in informatics do not benefit from the deficit of internal legislation on the one hand and the absence of international agreements that address the protection of the international community from the consequences and effects of these crimes.

The second is the difficulty of discovering and establishing an information crime: Not to leave this type of crime with any external impact after its commission is behind the difficulty in detecting it. In addition, the criminal's ability to destroy the evidence of conviction in a short time is an additional factor in the difficulty of detecting this type of crime.

And the third is the difficulty of proving cybercrime**:** One of the practical difficulties facing investigators is that cybercrime does not leave clear traces and the expert or specialist only who can detect, track and prove them (Maryam, 2013, p.12), and the reason why it is difficult to prove these crimes is that the criminal erases their effects, and the effects that reached them.

Discovering an information crime is something as we have mentioned before - not easy, but even if this crime is discovered and reported, then proving it is surrounded by many difficulties as well.

Cybercrime takes place in an unconventional environment where it falls outside the framework of the tangible physical reality, so that its pillars are found in the computer and internet environment, which makes matters more complicated for the security authorities and the investigation and prosecution authorities. In this environment, the data and information are invisible electronic pulses that pass through the information system, which makes red erasing the evidence entirely by the subject very easy.

In one of the cases in Germany, one of the criminals entered the computer system security instructions to protect the data stored inside it from attempts to access it that would completely erase this data by an electric field, if it was penetrated by others.

It should be noted that the means of inspection and their traditional methods often do not succeed in proving this crime due to its special nature, which differs from the traditional crime.

ISSN: 2616-9185

The latter has a theater on which events take place, as it has material effects on which evidence is based and this theater gives the way to the authorities of inference and criminal investigation to uncover The crime, by examining and preserving the material effects of the crime. But the idea of a crime scene in information crime is less than its role in disclosing the facts leading to the required evidence for two reasons[(2)]: The information crime does not have any material consequences , and Many people return to the crime scene during the period from the time of the crime until its discovery or investigation is a relatively long period, which gives room for the criminal to change or tamper with the physical effects, if any, which raises doubts about the significance of the evidence taken from the examination in the crime Informatics.

In addition, the lack of technical expertise of the police and the judiciary is an essential obstacle to proving information crime, and that this type of crime requires training and qualification of these entities in the field of information technology and how to collect evidence, inspection and prosecution in the computer and internet environment, and as a result of a lack of experience and training a lot Whatever the police forces fail to appreciate the importance of the information crime, they do not exert efforts to expose its ambiguity and arrest the perpetrator of efforts commensurate with this importance. Rather, the investigator may destroy the evidence for the existence of the contents of the hard disk in error, negligence in dealing with floppy disks.

2.2.2. a disappeared crime scene

The crime scene is the place where the roles of criminal activity have ended and the activity of the criminal investigator and his associates begins.

With the intent to search for the criminal from the reality of the effects he created at the crime scene, which is like a silent witness, who, if the criminal investigator did better in dealing with him, obtained certain information that would contribute in a large way to revealing the truth, (Sagheer, p.14), but the cybercrime scene is completely different from the traditional crime scene If the latter is located in a concrete reality and certain limits, then cybercrime falls in a virtual reality that has no limits. This creates many real and legal problems for investigators. After the emergence of information networks, there are no longer visible or tangible borders that stand in the way of transferring information across different countries.

ISSN: 2616-9185

The ability of computers and networks to transfer information and exchange it between systems separated by thousands of miles has led to the possibility of crime occurring in multiple places at the same time. The movement of information through modern technology systems made it possible to commit a crime through a computer located in a particular country while a criminal act was being carried out in another country.(Al-Momani, 2008, p. 3)

This characteristic of information crime as a cross-border crime has created many problems about determining the state with jurisdiction over this crime, as well as about defining the law to be applied, in addition to problems related to prosecution procedures, and other points raised by cross-border crimes in general How can members of the unprepared and unprepared police officers follow up on the accused in this disappeared theater, and they may be outside the virtual territorial scope of the state?

The issue of jurisdiction throughout the virtual world is one of the problems facing jurisprudence, which revealed the deficiency of general procedural rules. The reason for this is that the Internet is not subject to the authority of a particular person or country, and therefore we have multiple procedural laws that can control this type of crime by multiple states associated with it. Jurisprudentially correct that the principle of territoriality of the criminal text must be adhered to, taking into account precautionary principles, while the Budapest Convention in its Article No. (٢٢) affirms that each state must punish for the commission of these crimes even if the criminal is outside the territory of the state, so it is considered Jurisdiction is held if the computer system in question is inside the territory of the state and is outside it, or the computer system of the victim is within the regional domain, or the source of the transmission or destination is within the territory of the state. The fourth paragraph of the aforementioned article also indicated that the parties may take other forms of standards of jurisdiction in a manner consistent with their internal law (Abdul Raouf, 2011, p. 200), and if the crime in an electronic environment falls within the jurisdiction of more than one country, these countries consult with each other to determine the appropriate place for trial in order to avoid duplication Specialization.

ISSN: 2616-9185

The American judiciary has resorted to solving the problem of jurisdiction by relying on the principle of personal jurisdiction, which makes the US courts competent to consider cybercrime, in two cases: When the perpetrator is in the territory of the state, and: When the perpetrator has a minimum level of contact within the state. (Abdul Raouf, p. 209)

3. models for cybercrime devices "Internet police"

In the face of the increase in cybercrime on the one hand, and the inability of the judicial seizure bodies to investigate and expose their perpetrators on the other hand, many comparative legislations have directed towards adopting special devices for research and investigation in cybercrimes

Yes, cybercrime has brought emergencies to the judicial and investigation systems. Therefore, there is a need to create special devices for these crimes that are completely different from the regular seizure devices, (Hisham, Farid, 2000, p.45) which made the Budapest Convention for Information Crime advocating the necessity of creating such devices at the national level (Hirwala, 2007, p.104) and legislating the necessary legislative procedures for that, as stated in its Article (14) that: Each party may adopt legislative or other procedures that it deems necessary in order to establish authorities and set the procedures stipulated in this section for the purpose of special criminal techniques or procedures(3) The agreement allows each party to reserve the right not to apply the measures referred to except to a specific class of crimes. (Hilali, 2001, p.174)

3.1. models for Internet police in comparative legislation

3.1.1. In the United States of America

Among the developed countries in the field of creating special devices for searching and investigating cybercrime, the United States of America has created a large number of specialized units. Among these units, you find the Central Office for Combating Crime linked to Information and Communication Technology, as well as the Computer Crime Section of Intellectual Property Rights Crime, which was established in (1991), and its members have reached 20 prosecutors in the year (2000), (Hirwalaa, 2007, p.10) and we also find the Computer Security Institute and a

ISSN: 2616-9185

Crime Unit The Internet is a unit that specializes in high-tech crime and is run by an FBI assistant director. (Hirwalaa, 2007, p.11)

There is in the state of Ohio in the United States one of the international organizations that aim to protect websites from hacking operations The Internet Police (police internet) where this organization works to protect the sites that it contracts with officially, in exchange for money by preventing any attempt to penetrate a protected site From her side. And if the attempt is repeated more than once by the same cybercriminal "hacker", the part responsible for communicating with the Internet is frozen so that the computer system fails to communicate with it, and among the sites protected by this organization we find some e-commerce sites from the Internet, and a site Federal detective, sites of the Ministries of Interior and Defense.

3.1.2. in France

The French legislator created the central office to fight crime related to information and communication technology. This was in accordance with ordinance No. (405/200) at the level of the Central Directorate of the Judicial Police(4), and the Internet Section of the Technical Department for Legal and Documentary Research was established in (1998), which is a department of the National Gendarmerie and consists of (13) person among the engineers and technicians and this department is in charge The task of processing information, and performing complex electronic searches. We also find the information section of the Criminal Research Institute in the National Gendarmerie. Who established the year (1992) and its mission is to provide technical assistance in the form of experience, interception or oversight, as well as analysis of data integrated into computers, especially those related to electronic and financial commercial transactions. (Hirwalaa, 2007, p.139)

Among the competent authorities in France, we also find the central office to combat crime related to information and communication technology, which was established by ordinance no. (405/200) and is present at the level of the Central Directorate of the Judicial Police(5). There are three units used by the office to carry out its tasks, which are the operations unit and it consists of four teams dealing with crimes of fraud by means of payment as well as crimes on communication networks, and the unit of technical assistance,

Which is a unit equipped with advanced technology means programs. It facilitates judicial interventions, while the Scientific Documentation and Analysis Unit handles the information obtained from space activities(6).

3.1.3. The necessity of international cooperation

The necessity of international cooperation in the field of creating devices specialized in cybercrime, because a country that wants to succeed in facing cybercrime can only cooperate and coordinate with other countries. It is necessary to have international cooperation in the field of training men of justice(7) , as training of human cadres is not the same in all countries, but it differs depending on the progress of the state or not, and if we looked at some international or regional legislation, we found that it called for the need for cooperation between countries in the field of training and transfer Experiences with each other(8) .

And it is required that the trainer have the scientific authorities and mental and psychological abilities in order for the training to bear its fruits, and some authorities require that the training recipients have sufficient experience in the fields of computer operations, programming, system design, analysis and project management. Among the most important elements that the qualification must receive is to know everything related to the risks and threats to the computer system as well as the types of crimes arising from its misuse, then the most important procedures for investigation, research and planning, how to collect and analyze information, methods of facing cyber-attacks and how to control them The training also ensures the identification of evidence in the electronic field, as well as inspection and seizure procedures(9) .

Algeria is also striving to develop its judicial police services, as CIA experts and FBI agents supervised a yearly training workshop (٢٠١), which was about combating information crime for the benefit of judicial police officers and judges. It aims to acquaint them with the latest technologies in combating crime and how to use electronic evidence for investigation and prosecution. Experts in the training workshop participated in computer crime and intellectual property, And the Department of Organized Crime and Blackmail of the US Department of Justice. This training workshop benefited about (10) officers from the judicial police and (60) specialized in organized crime in Algeria.

ISSN: 2616-9185

The training focused on both theoretical and practical aspects, as were the identification of techniques for investigative procedures and the establishment of evidence on information crime, the relationship of information crime to organized crime, information security and data, and how to exploit the Internet and e-mail, as well as international cooperation in this field[(10)].

The truth is that no country, no matter how much progress and development, can face these emerging patterns of crime alone, therefore there is no escaping the strengthening of international cooperation in the procedural aspect, and these countries are inevitable to provide assistance to developing countries to strengthen their institutions specialized in the investigation.

4. Conclusion and recommendations

Finally, we can say that cybercrime is distinguished from the rest of the known traditional crimes, because this matter is naturally due to the characteristics of this crime and these characteristics are that the computer and technical systems are an element in its implementation, therefore, the detection, investigation and proof of cybercrime is an order Difficult. What makes this more difficult is that it is a phenomenon that has broken geographical barriers and has overcome all the rules governing the spatial concept of crime. Therefore, it is a crime that does not recognize borders. You may find every element of the crime in a certain place or the region of a particular country. As a result, the damage and losses caused by this crime are very high and constantly increasing when compared to traditional crimes. As a result of the foregoing, the person who commits these Crimes is somewhat distinct from traditional crime criminals.

We are not in front of a thief or a fraud, or an ordinary fraudulent, but rather in front of what is called an information criminal, and in addition to enjoying the characteristics of an ordinary criminal, we find that he possesses a kind of intelligence and knowledge of the most recent digital technology that creates the environment for the practice of criminal activity, and on the other hand he must have The skill required to carry out a criminal activity that stems from his possession of a measure of knowledge and skill that he may acquire as a result of his studies or practical experience in this field, and in most cases, we find that it is distinguished by a variety of motives between revenge, material gain, curiosity, challenge, terrorism, blackmail, or Political ...

ISSN: 2616-9185

etc. Consequently, these criminals find them to be described with special and specific designations that result in the presence of many denominations for them that specialize in every art in the practice of certain activities pirates or virus makers or imitators of programs and others.

On the other hand, the reality of these crimes has resulted in new, previously unknown, innovative crimes or traditional crimes being committed in a new way. In this scope, many efforts have been made to classify cybercrime, whether at the individual effort of the jurists or at the level of international or regional organizations. Whereas, the cybercrime have proven to be crimes that cannot be enclosed in parentheses and as a result of the characteristics referred to previously, they are classified into four sects: crimes against people, crimes against trust and the public interest, crimes against money, and crimes against state security, organizations and institutions. Of course, under each sect there are many sects that represent criminal activities that violate the correct construction of society and threaten its existence, and this division stems from the principle of interest that the legislator has sought to protect. And as you found out, we tried to develop a classification capable of accommodating any developments in this scope and understanding the status of these crimes, especially as they are related to the computer and information technology that have different roles in the implementation of the crime.

And based on the foregoing, Even if the state prepares the ways and material and human capabilities to confront a crime, limiting this crime and arresting its perpetrators will not come unless this willingness is commensurate with the nature of the crime. Cybercrime is fundamentally different from other crimes, in terms of its composition, commission, effects, scope and even perpetrator, so it is not possible to search and investigate only those who have knowledge of the nature of these crimes and who are capable of information, communication and information technologies, and from here require the legislator the following:

1- The necessity of forming judges specialized in information and communication technology crimes.
2- The necessity of forming the regular police members in the field of information and communication and providing them with the necessary ways, to uncover cybercrimes as a proactive step until creating a special device.
3- Establishing specialized centers to study this type of crime.

4- The necessity of international cooperation in combating cybercrime and building specialized entities in research and investigation.

5- The necessity to attract cybercriminals to work as assistants for seizure members.

Endnotes:

(1) Each party must also apply the authorities and procedures referred to in paragraph 1 to the criminal crimes set forth in accordance with Article 2 to 11 of the Convention, which are crimes that affect the confidentiality and integrity of the availability of data, information systems, computer-related information crimes, and crimes against property Intellectual and all criminal crimes installed through an information system ..., see the second paragraph of the above-mentioned article.

(2) Among the reasons that prevent the discovery of this type of crime, is the refusal to report to the victim, as most of the entities whose information systems are exposed to violation or suffer heavy losses due to lack of detection in order to avoid damaging their reputation and standing and shake confidence in their efficiency. For more, see Nahla Abdul Qadir Al-Moamni, Information Crime, an article published in the year ٢٠١٢, and accessed on 7/١١/2019 at the evening on the following site: http://kenanaonline.com/users/ahmedkordy/posts/409974

(3) The second paragraph of the article indicated that each party should apply the authorities and procedures referred to in paragraph 1 to criminal crimes in accordance with Article 2 to 11 of the Convention, which are crimes that affect the confidentiality and integrity of the availability of data, information systems and computer-related information crimes, And crimes against intellectual property and all criminal crimes committed through an information system.

(4) This office uses three units to carry out its tasks. The first unit, the operations unit, consists of four teams that specialize in fraud crimes by means of payment, as well as crimes on communication networks. The second unit in the technical assistance unit is a unit equipped with advanced programs and technological ways, working on Facilitating judicial interventions in the internet, while the Scientific Documentation and Analysis Unit is working to process information resulting from space activities

(5) The office is supported by the Ministry of Defense, Economy, Finance, and Industry.

(6) It indicates that the central office to combat crime related to information and communications technology consists of 3 policemen and 3 men from the National Gendarmerie and is constantly increasing as needed.

(7) As this process aims to change their behavior and raise the level of their skills and attitudes, in a manner that ensures proper completion of the legal, judicial and executive work. ., See Hussain bin Saeed bin Saif, International Efforts to Confront Cyber Crime, article published on 2014, It was viewed on: 25/12/2016 at 8 pm on the following site: www.minshawi.com

(8) See, for example, Article 29 of the United Nations Convention against Organized Crime of 2000 AD, and Article 9 of the draft Arab Convention against Transnational Organized Crime.
(9) It is worth noting that the United States has an office for assistance, training, and public prosecution services abroad. It is affiliated with the US Department of Justice, specifically charged with providing the necessary assistance to strengthen criminal justice institutions in other countries and strengthening the administration of justice abroad. The US Department of Justice also provides assistance to develop the Judicial sector in a number of countries in Africa, Asia, Eastern and Central Europe, Latin America and the Caribbean, and newly independent countries, including Russia and the Middle East, drawing on the expertise of their specialized units. See Hussain bin Saeed bin Saif, op. Cit., At the following website: http://kenanaonline.com/users/ahmedkordy/posts/409974
(10) On the other hand, the US ambassador to Algeria, David Pearce, said on that occasion that Washington is interested in establishing a more effective partnership between Algeria and his country in combating information crime, as it is useful to know the behavior of the crossroads of this crime in different countries., See, Othmane Lahyati, a workshop on cybercrime and information security, an article published on 2015, and the article was reviewed on 12/17/2016 at 7 pm on the following website: http://www.clkhabar.com/ar/index.php?news-235287

References:

1. Abdul Raouf, Tariq Muhammad (2011), the Crime of Fraud through the internet, Al-Halabi Publications: Beirut Edition.
2. Ahmad, Abdullah Hilali (2011), Budapest Convention for the Suppression of Information Crime, Arab Renaissance House, Cairo.
3. Al-Momani, Nahla Abdul Qadir, Information Crime, article published on the following website: http://kenanaonline.com/users/ahmedkordy/posts/409974
4. Al-Momani, Nahla Abdul Qadir (2008), Information Crime, The House of Culture for Publishing and Distribution, First Edition, Oman.

5. bin Saif, Hussain bin Saeed, International Efforts to Confront Cyber Crime, article published on the following website: www.minshawi.com
6. Budapest convention for Information Crime of the year (2001).
7. Dr. Francillon, (1999), Computer crimes and other crimes in the field of computer technology in France.
8. Hirwala, Heba, Nabila (2007), Procedural Aspects of Cyber Crime, University House of Thought, Egypt.
9. Khaled, Younis, Mustafa,Arab (1994), Computer Crime, a comparative study, Master Thesis submitted to the University of Jordan.
10. Maryam, Masoud Ahmed (2013): Mechanisms for Combating Crime of Information and Communication Technologies in the Light of Law No. 04/09 Memorandum for Master's Degree, Faculty of Law, University of Ouargla, Algeria.
11. Mourad, Abdel-Fattah (2007): Criminal Technical Investigation, Alexandria.
12. Muhammad, Hisham, Rustom,Farid (2000), procedural aspects of information crime. Library of Modern Instruments, Egypt,.
13. Othmane Lahyati, a workshop on cybercrime and information security. Article published on the following website: http://www.clkhabar.com/ar/index.php?news-235287
14. Sheta, Mohamed (2001), the idea of criminal protection for computer programs, the new university publishing house, Alexandria.
15. The Arab Convention against Information Technology Crimes, ratified by Presidential ordinance No. 14/252 of September 8, 2014 on an official journal, No. 57.

16. Yusef, Sagheer Crime committed online. Memorandum for a master's degree in law, Faculty of Law and Political Science, Mouloud Mamari University - Tizi Ouzou, Algeria.