PalArch's Journal of Archaeology of Egypt / Egyptology

INTERNATIONAL EFFORTS TO COMBAT CYBERCRIME

Dr. Baqer Musa Saeed AL_khafagy

Department of Law, College of Law, The Islamic University, Najaf, Iraq

Corresponding Author: baqer.musa@iunajaf.edu.iq

Abstract

Today, we are living in the period of data and correspondence innovation, which has become the premise on which all fields rely upon, and for all establishments, regardless of whether they are public foundations claimed by state governments or private organizations possessed by people, the data innovation in the administration of administrations and correspondence networks is the essential device on the way.

This has been the quick advancement of data and correspondence innovation and the Internet has driven the entire world to the rise of new examples of wrongdoings got through the misuse of the innovation, which came about with the formation of another criminal marvel, a wrongdoing identified with robotized computer and the Internet, which is made by assaults and forward leaps and penetration inside Information frameworks with the end goal of either pulverizing those frameworks or acquiring private data, regardless of whether military or financial, which cautions that there are hazards at the worldwide and public levels if this wonder isn't tended to, which will bring about military and social misfortunes, on the off chance that they are left to the general public. This requires - and this is the situation - discovering approaches to address this wonder. Digital crimes are violations over the Internet that depend on invasion into unapproved sites to enter, with the point of disturbing or crushing the information accessible on them or holding onto them, and it is a progression of digital assaults did by another state.

Keywords: Efforts, combat and cybercrime.

Introduction

It is recognized that we are living today in the era of information and communication technology, which has become the basis on which all fields depend on, and with all institutions, whether it is public institutions owned by state governments or private institutions owned by individuals, the information technology is the tool for managing the affairs and networks. Countries and the provision and facilitation of services through them.

This has been the rapid development of information and communication technology and the Internet has led the whole world to the emergence of new patterns of crimes came through the exploitation of the technology, which resulted with the creation of a new criminal phenomenon, a crime related to automated computer and the Internet,

which is made by attacks and breakthroughs and infiltration inside Information systems with the purpose of either destroying those systems or obtaining confidential information, whether military or economic, which alerts the existence of risks at the international and national levels if this phenomenon is not remedied, which will result in military and social losses. The world. This necessitates - and this is the case - finding ways to address this phenomenon.

Cyber-crimes are crimes over the Internet based on infiltration into unauthorized websites to enter, to disrupt or destroy the data available on them or seizing them. It is a series of cyber-attacks carried out by another state. The distinguishing characteristics of the Internet are that it does not know the international borders. The user of the Internet can move between the parts of the world while he is in his place in front of the computer screen or the mobile phone. It follows from the international nature of the Internet that the crimes that are committed through it have the characteristics of international crimes or transnational crimes. It is possible for more than one person in more than one country to participate in committing a single crime in which several individuals residing in multiple countries fall victim to the matter. The Mashreq, Morocco and the Islamic world may transmit information or pictures on the Internet that may be legitimate in the country of its origin, but which may have been unlawful in another country. Also, the different legislation in establishing criminal jurisdiction because of the multiplicity of the foundations of this jurisdiction may lead to a conflict of jurisdiction between states for Internet crimes cross-border, a crime may be committed in the territory of a particular country and the perpetrator a foreigner, are governed by this The crime is subject to the criminal jurisdiction of the first country based on the principle of territoriality, and it is also subject to the jurisdiction of the second state based on the principle of personal jurisdiction in its positive aspect .[1]

The crime committed on the territory of a state is one of the crimes that threaten the security and safety of another country, and it is subject to regional criminal jurisdiction on the one hand, and on the other hand the jurisdiction of the state of the victim on the other hand. The idea of a conflict of judicial jurisdiction also arises if jurisdiction is established on the principle of territoriality as if the perpetrator broadcasts illegal information or pornographic images from the region of a specific country and the jurisdiction has been seen in another country, according to the regional jurisdiction. The impact of the crime, whether the act of broadcasting or the result of the act occurred. Here, we find that the matter will violate the principle that it is not permissible to prosecute a person for a single act more than once, which is one of the basic principles on which the Criminal Law is based.[2]

More than that, the cybercriminal may be a person in general international law, and a state may commit cyber crimes against another country to obtain scientific, economic, or military information, or depriving the state of possessing such information. The loss of confidence in the state due to its inability to obtain the required protection.

Research importance

Combating cybercrimes and cybercrime has become extremely important for us to look into the ways that must be followed to address these transnational crimes, which require the identification of their nature, characteristics, criminal nature, characteristics of their perpetrators, and their perpetrators. It is also imperative that we research the methods and procedures of international cooperation that are consistent with the nature of crimes related to the information network and which are of a special nature that requires that there be quick responses to cybercrimes. The spirit of cooperation between the internal legal systems of countries.

Research problem

The problem raised by this research and which requires searching for an answer is: Is there a special nature of cybercrime that differs from conventional crimes? Is the cybercriminal different in terms of characteristics and criminal objectives from the traditional criminal? And if the perpetrator of the crime is one state against another, does the aggressor state ask international criminal and civil liability for that crime? Is this crime an international crime? And are there legal ways and means that have been taken internationally to counter the cyber-attack? And if the countries of the world have taken the means they have to reduce cybercrimes, have these means found the international cooperation required to activate them, or are there obstacles in this regard that prevent access to the reduction of cybercrimes?

The first requirement

International cooperation between police services

The great development in means of transportation in general and the information network, in particular, has resulted in the movement of criminals from one country to another. The international community has realized that it has become impossible for any country to eliminate transnational crimes because the general procedures of the police services in each country do not make its security apparatus track down criminals and pursue them if they cross the borders of states. Accordingly, the need for police services to cooperate and coordinate action among them to chase criminals.

First - Connecting communication and information networks

Communication takes place between the national criminal justice agencies in general and the police services in particular, and between those agencies in other countries through the diplomatic corps, as police communications need special communications to achieve the required speed. Therefore, the International Criminal Police Organization (INTERPOL), as well as many countries, tried to develop communication systems and exchange information between them, so that the criminals could arrive and track down as soon as they left the country in which the

crime was committed. To pursue the prosecution of criminals within the borders of the country from which he fled.[3]

Second - International Criminal Police Organization (INTERPOL)

INTERPOL is considered the most important international police cooperation mechanism to combat global crimes that cross national borders in general and cybercrime in particular. INTERPOL's main mission is to activate cooperation between the police authorities of member states in the organization and to initiate and standardize extradition procedures, and through coordination of police work, collecting data and exchanging information to facilitate investigation services, to arrest and prosecute criminals and to persecute them. Prevention and Punishment for Common Law Crimes .[4]

This task is entrusted to the central and national offices in each member state and a permanent body appointed by the national government authorities, and with the assistance of INTERPOL, teams to move about events that can facilitate a set of investigation services for public investigation and investigation. The Interpol to circulate warnings and alerts included intelligence briefings and advice analytical and technical for potential criminal threats and uses INTERPOL tools own as a system of international releases of various kinds and investigation databases and provide expertise and training courses in the field of combating cybercrime, using a group of international experts and laboratories At the global level, and facilitating the exchange, analysis and storage of criminal data, as the organization provides the State Parties' police with guidebooks about cybercrime and how to train to combat it and investigate it. Technology-related financial crime is one of the main crimes of INTERPOL .[5]

Third - Mutual assistance to cope with disasters and crises

In the event of a crisis and critical situations, the element of time is one of the decisive matters in confronting that crisis or disaster, which requires intensifying and increasing efforts, experiences, and capabilities in the international effort. Rescue and civil defence forces for countries affected by earthquakes, hurricanes and floods, or to participate with experts or provide advanced equipment. Likewise, the participation of special forces, experts, or equipment in releasing detained hostages, or important occupied buildings, or hijacked planes or ships.[6]

Fourth - Carrying out some joint international police operations

Examples of this are controlled delivery in the field of drug control, which means allowing an illegal shipment to pass under control through a region, as well as a hot pursuit in other countries, which is intended to track down the other victims.

Fifth - manifestations of police cooperation at the international level in combating cybercrimes

1. International Web Police:[7]

This organization was established in the United States of America in 1986 to receive complaints from users of the network, prosecute perpetrators and pirates electronically, search for evidence against them, and present them for trial. Given the expansion of this organization's activities and the procedures it carries out in cooperation with law enforcement agencies in the member states, this makes it easier for the work team to track the criminal activities that are committed through the Internet on the Internet. In the context of the issue of legal controls that govern the flow of information over the Internet, some think that it is necessary to set controls and rules so that they do not lead to prejudice to public freedoms in the exchange of information and human rights to human rights. On the other hand. The researcher believes that the problem is not in blocking pornographic pictures and sites, but rather than sites that broadcast ideas that corrupt society and call for demonstrations or coups under the so-called public freedoms and human rights, then the burning of human rights. The special interest.

However, the difficulty that Internet police agencies face when the crime is carried out through internet cafes, in which clients carry out whatever crimes they want without the ability to identify them, as these cafes do not require them to be identified by their clients. For example, the Federal Bureau of Investigation in the United States, after it tracked down a hacker, who penetrated the information network of a bank, but it was not able to identify and prosecute him. Because it was found that he carried out his operation through several internet cafes. To solve the problem the researcher believes that the states bind should the owners of Internet cafes to prove personalities the cafe before entering in addition to the presence of surveillance cameras the details of showing the face of all the cafe does not depend on personal proof only because it is possible that the data contained in the personal forged investigation. The cameras determine the user's person.

2. Internet Fraud Report Center:[8]

This centre was established in the United States of America on 5/2000/18 to cooperate with the FBI and the National White Collier Crime Center, to receive reports and track the crimes and violations of the network of fraud. The relevant control and control agencies inside and outside the United States of America through the centre's website on the international network. To tighten control over the Internet, the United Arab Emirates has implemented what is known as a proxy system, which reviews the quality of services provided over the Internet. When the subscriber requests a site on the parent network, the sign arrives at the censor, who in turn displays the subject on a very large list of prohibited sites. If it appears to him that the requested site is included in this banned list, then he does not know that the requested site is included in this prohibited list. This website was banned by the Emirates Internet regulator.

The second requirement

Cooperation of the judicial authorities of countries

International judicial cooperation balances between the independence of the state in the exercise of its criminal jurisdiction on the borders of its territory, and the necessity to exercise its right to punishment.

- The first reason: The state abides by its territorial borders. The penal code may extend its application beyond the borders of the state's territory. However, measures cannot be undertaken outside the national territory because their practice violates the sovereignty of other foreign countries.
- The second reason: Penal law cannot be applied without criminal procedure law. Criminal procedures are the necessary means to implement the penal code and move it from a state of inactivity to the movement. It is necessary to resort to judicial cooperation (to overcome this difficulty), and this cooperation is represented in a group of means by which one of the auxiliary states provides its public authorities or judicial institutions to take control of the authorities or their judicial institutions.

Whereas cybercrime is global, and therefore its effects can encroach on several countries; The prosecution of the perpetrators of these crimes, bringing them to trial and punishing them, requires the conduct of procedural actions outside the borders of the state, such as inspecting, or seizing hard pirates in the case of unlawful witnesses or searches of the witnesses on whom there is information from the witnesses or the searches of the units. A judicial authorization or providing information that could contribute to the investigation of crimes. All of this will not be achieved without the help of other countries.

Legal aid takes several forms[9]

1. Information exchange: This consists of providing information and documents requested by a foreign judicial authority in connection with a crime regarding the accusations that have been directed against its nationals abroad and the measures taken against them. The judicial authority knows precisely the criminal past of the person referred to it, as it helps in implementing the provisions related to recidivism, suspension of the execution of the sentence and incompetence.
2. Transfer of procedures: The transfer of procedures means the state, based on an agreement, to take criminal procedures in connection with a crime committed in the territory of another country and for the benefit of this state, if the following conditions are met:

A. That the act attributed to the person constitutes a crime in the requesting state and the requested state.
B. Any contracting party may request any other party to take penal measures in any of the following cases:

- If the accused person is subject to or will be subject to a ruling restricting freedom in the requesting state.
- If the actions to be taken are decided in the law of the country from which he is requested for the same crime.
- That the required action leads to reaching the truth, such as if the evidence of the crime in the requested country.
- If the execution of the judgment is in the requested country, it will achieve the social rehabilitation of the sentenced person.

- If the presence of the accused person at the hearing cannot be guaranteed in the requesting country, while his presence in the requested country is guaranteed.

3. The requested State may refuse to transfer the procedures in the following cases:

- If the request to transfer the measures is not justified by the fact that the reasons mentioned by the requesting state do not call for taking such measures.
- If it is proven that the motive behind the request to transfer the procedures is racist, religious or political considerations.
- If the requested country had applied its law to the crime before it was received from the requesting state and the procedure that was previously taken conformed with the law.
- If the procedures required by the requesting state violate the obligations of the requested country
- If the required procedures violate the basic principles of the legal system in the requested country.

However, there is an opinion that, and rightly so, that the application of these traditional mechanisms from the agreements raises some problems, such as the existence of obstacles specific to crimes committed over the Internet, even if those obstacles exist at the local or national level, but they are also raised (at the level of states). Among these obstacles, electronic communications are traced through the investigation authorities and evidence is established for crimes committed in the field of the Internet, given the differences that exist between the different legislations regarding the conditions of admissibility of evidence, such as the enforcement of evidence, and the enforcement of actions.[10]

4. International judicial delegation:

Judicial delegation is one of the forms of judicial assistance for international punitive cooperation, as it enables one country to benefit from the public authorities of another country if the regional borders prevent it from enforcing its law towards the criminal.

By international judicial delegation, we mean a request to take a judicial action from the criminal case procedures that the requesting country presents to the requested country because of the necessity for that to decide a matter before the judicial authority in the requesting state, and he can't be censured. Accordingly, the judicial delegation is a procedure to facilitate the criminal procedures between countries to ensure that the necessary investigations are carried out to bring the accused to trial, and to overcome the regional sovereignty obstacle that prevents foreign countries from practising some of the internal judicial acts. Examples include hearing witnesses and procedures for conducting the criminal case .[11]

Judicial delegation is carried out between countries through agreements that contain the conditions and methods of implementing judicial delegation. Those who leave the state with the discretionary power to

implement or not implement what is requested of it, for fear that its responsibility will be internationally neglected.

The third requirement

International conventions in the field of combating cyber crimes

International agreements and treaties are one of the most important forms of international cooperation in general, and in the field of combating crimes resulting from cybercrimes in particular. Among the treaties and agreements that work on international cooperation in the field of combating cybercrime, the Budapest Treaty to combat Internet crime, and the recommendations of the European Council on the problems of criminal procedures related to information technology, and we explain them in the following:

First - Recommendations of the European Council[12]

The rapid development in the field of computer and Internet technology and the European countries' feeling of the importance of reconsidering the penal procedures in this field led to the European Council issuing Recommendation No. 13/95 on 9/1995/11 regarding the problems of criminal procedures related to technology and information technology. National penalties, to match the development in this field, and among the most important things mentioned in the recommendation of the European Council are the following:

1. The laws shall clarify procedures for inspecting computer equipment, controlling the information it contains, and controlling the information during its transmission.
2. That the national criminal procedures allow the inspection bodies to control the computer programs and the information in the devices by the same conditions for the regular inspection procedures. The inspection
3. During the inspection process, the executing bodies and concerning the established guarantees shall be allowed to extend the inspection to other computer systems in their area of competence that is related to the system subject of inspection and to control the information in this procedure, provided that this is done.
4. The Criminal Procedures Law clarifies that the procedures for traditional documents apply about the information on computers.
5. Surveillance and registration procedures shall be applied in the field of a criminal investigation, in case of necessity, in the field of information technology. Confidentiality and respect must be provided for the information that the law imposes special protection for.
6. Personnel of governmental and private institutions that provide communication services in cooperation with the investigation authority must be required to conduct monitoring and registration.
7. Procedural laws must be amended by issuing orders to whoever possesses the information, whether it is programs, databases, or data, related to computer equipment to hand it over to reveal the truth.
8. The investigation authorities should be given the authority to direct orders for those who have private information to enter an information system or to

access the information it contains to take the necessary steps to allow the investigation personnel to access it. And to authorize the investigation authorities to issue similar orders to any person who has information by way of operating and preserving the information.

9. The systems for dealing with electronic evidence must be developed and standardized, and for it to be recognized among the different countries, the procedural texts of traditional evidence must also be applied to electronic evidence.
10. Special units must be formed to combat computer crime and special programs should be prepared to qualify criminal justice workers to develop their information in the field of information technology.
11. The investigation procedures may require extending the procedures to other computer systems that may be located outside the country and assume rapid intervention, and so that this matter does not constitute an assault on the sovereignty of the state and international law, an explicit legal rule must be established by you. When and how to take such actions.
12. There must be quick and appropriate procedures and a communication system that allows the investigative bodies to contact a foreign party to collect specific evidence, and the last authority must then allow inspection and seizure procedures. This authority must also be allowed to conduct records of current transactions and determine their source. Therefore, existing international cooperation agreements must be developed.

Second - The Budapest Treaty to Combat Internet Crime[13]

The Budapest Treaty to Combat Cybercrime is the first of the treaties related to those crimes that were concluded in the Hungarian capital Budapest on 11/23/2001, which highlights international cooperation and solidarity in the fight against cybercrime. Which is carried out over the Internet and bad use of it.

That treaty has been signed by 26 European countries in addition to Canada, Japan, South Africa, and the United States of America. The treaty provides the foundations for public security and includes 48 articles in four chapters as follows:[14]

Chapter One: Definitions of some technical definitions

The second chapter includes the measures that need to be taken at the local level for each country, and they are divided into two parts:[15]

- The first section: relates to substantive criminal texts as follows:

1. Concerning crimes against privacy, the integrity and existence of computer information and computer systems, and it includes a description of multiple types of crimes.
2. Computer-related crimes, including the use of computers for forgery and fraudulent acts.
3. Crimes related to content and content.
4. Crimes related to copyright infringement.

- The second section: the procedural law about the criminal procedures, including the preservation of stored information and orders related to the

delivery of evidence, and also includes the inspection and control of stored computer data.

- Chapter Three: Issues of international cooperation, extradition of perpetrators, joint support and cooperation in investigations and collecting traffic and movement data on data.
- The fourth chapter relates to joining and withdrawing from the treaty amendment, dispute resolution, and consultation among members.

Even though this treaty is European in origin, it is open to other countries to request joining it, so that the benefit from them will be circulated to all countries.[16]

This treaty has dealt with crimes that are considered among the most common crimes worldwide, such as electronic terrorism, credit card fraud, and child prostitution. The treaty also specified the methods to be followed in the investigation of cybercrimes, and the signatory countries pledged to cooperate to fight them. The treaty also tried to establish a balance between the proposals made by the police apparatus, and what the human rights organizations and Internet service providers expressed from concern, as human rights organizations fear that the freedom of the treaty will be challenged and that the human rights organizations will limit the freedom of the treaty.[17]

Fourth requirement

Hand over the accused to justice

The ease with which the accused escape from being subjected to punishment in cybercrime, and the inability and difficulty of pursuing them have led to the necessity for states to resort to the path of extradition and follow the criminal wherever it was in order not to escape punishment and thus combat cybercrime and its cybercrime. These criminals remain with impunity, doing whatever they want. In the context of a conversation about the system for the extradition of the accused, we will talk about the concept of this system, its conditions and procedures in general, and then we will follow that by talking about the system for the extradition of accused in the field of cybercrime and that:[18]

1. First - in the concept of the extradition system: The system of extradition of accusers is "an international cooperation procedure whereby a state called the requested state extradites a person who is in its territory to a second country called the requesting state or an international judicial body, intending to prosecute him for a crime (he has committed a criminal offence)."

Accordingly, the idea of extraditing the accused is based, on the one hand, on the existence of a relationship between two countries. The first state demands that the perpetrator of the crime extradite to it to take the necessary measures against him, and the second country does not direct the request for extradition in it if a decision is made to him after he has been issued. An agreement between the two countries, and either the rejection of the absence of that legislation or that agreement. On the other hand, we find

it includes two groups of people. The first group is the group of accused persons who are accused of committing crimes, but no court rulings have been issued against them yet. They fled to another country. So surrender is of three types: administrative, judicial and mixed delivery .[19]

2. Second - Conditions of the extradition system:[20]

Some conditions must be met for the system of extradition to be enforced. The importance of these conditions is that they separate the boundaries of the relationship between the states parties in the extradition process and lay down the general provisions based on which the extradition will take place or not. If these conditions are met, the surrender decision will be made. These conditions are almost identical in all cases of extradition in terms of the elements, as for the subject matter they are the subject of disagreement between countries and that according to their need for delivery and the international interests considerations that each country takes into account:

1. Double criminality requirement: This condition means that the act for which extradition is requested is a criminal in the legislation of each of the requesting and extradited states. What is required here is that the act is criminal, regardless of the legal form or not. And to punish it, the legislation of the states may differ in the legal adaptation in which the crime is described, for example, if the act was punishable in the legislation of the requesting state under the name of the crime of investing money, while the same act was punishable in the future. This does not prevent the availability or dual criminality requirement. The condition of double criminality finds its basis in the fact that the state requesting extradition wants, from behind its request, to prosecute those who are accused of committing criminal behaviour or carrying out the sentence imposed on it. The penalty against the person of the accused, as it is not conceivable that a criminal judgment will impose a penalty on him, on the one hand, and the other hand, the State from which the extradition is requested cannot be required to impose a penalty for committing conduct of something wrong in the original law.

Most of the jurisprudence, which is supported by the researcher, goes to the fact that the requirement of double criminality may be an obstacle in the field of extradition. In national criminal legislation, we find that informational crimes are not punished in most other countries. The legislation of the requested country may or may not apply to crimes on computer networks and the Internet. In other words, it is difficult to search in the legislations of the countries whose extradition is requested, and whether their traditional criminal legislation can be applied to informational crimes or not, and thus the condition of double criminality is met or not. In addition to the fact that states may interpret the condition of double criminality broadly, which would impede the implementation of international agreements in the area of extradition of accused and prevent this from gathering evidence and prosecuting the perpetrators of internet crimes .[21]

Therefore, there must be coordination or unification between the various legislations about the definition of information crimes and cybercrimes, or at least not requiring dual criminality. This is also mentioned in the agreement concluded between Canada and America about mutual legal assistance that did not require double criminality as a condition for judicial cooperation between them and the interference of Internet crimes within the framework of this agreement .[22]

2. Conditions relating to the persons requested to be extradited: One of the established principles in the international community is that it is not permissible to extradite nationals, and most national legislation and international agreements have stipulated that. So if a person from the state commits a crime, it is not permissible to extradite him. Likewise, it is not permissible to extradite those who have been granted the right of political asylum, as there is an international consensus to exclude political crimes from the scope of extradition, whether on international agreements or national legislation. Likewise, if the person whose extradition is requested has been tried for the crime for which he is requested to be extradited, then he is acquitted or punished for it, then it is not permissible to extradite him. For it. This condition is considered one of the basic guarantees when trying the person whose extradition is requested, and it aims to provide the greatest possible degree of judicial protection for the person requested to be extradited to the requesting state so that this person is not subjected to a double-handed and double-handed contract. Such as the Arab League of Arab States Convention on the Extradition of Criminals, according to which Article (5) states that "extradition shall not take place if the person sought for extradition has been tried for the crime for which the extradition was requested, or for which he was exonerated or exonerated For which the delivery is requested in the country from which the delivery is requested ».[23]
3. Conditions related to the crime required to be extradited: There are three paths that many countries take to determine the nature of the crimes in which extradition is permitted, as follows:[24]

- The first approach: the inventory method or the list approach, and this method is based on the inclusion of a group of crimes based on exclusivity, for example (murder, swindling, theft, money laundering, ...) and these crimes are included in a list attached to the law or agreement. Only other crimes are the ones for which extradition is made, and this method is among the least common and widespread among the countries of the world, as it leads to the impunity of some criminals whenever the crime committed by them is not included in the list.
- The second approach: the method of the gravity of the crime or the minimum penalty. This method is the most common in determining the crimes in which extradition is permitted. It is for states to specify in their internal legislation or in bilateral or multilateral treaties or treaties that are mutually exclusive. Delivery for it.
- The third approach: the mixed system, which is also one of the common methods for determining the crimes for which extradition is permissible. This method has two benefits in terms of that it guarantees a certain degree of the severity of the crime for which one is punished in the country. They

represent a danger to the states parties for extradition without regard to the degree of their gravity or the penalty prescribed for them.

Third - procedures for the extradition system:

The procedures for the extradition of the accused mean those rules of a procedural nature that the states parties take in the extradition process by their national laws and their undertakings to complete the extradition process to reconcile the protection of human rights and freedom of human rights. A criminal of punishment. These procedures are shared by the country requesting extradition and the country from which the extradition is requested, and they are not absolute, but rather bound by some international or contractual obligations, and these procedures can be divided into two parts:[25]

1. Procedures of the country requesting extradition:

Where the country requesting extradition begins its procedures with the request and its desire to receive the person whose extradition is requested, the extradition request can only be moved upon a request submitted by the requesting state to the country from which the extradition is requested. The request is the instrument by which the requesting state expressly expresses its desire for the receipt of the requested person, and most international agreements on the extradition system stipulate that the request is submitted in writing, and the request for surrender must include the surrender of the accused and the request for surrender to him. Taken against him and clarification that the extradition request is in agreement with the assets.[26]

The state requesting extradition undertakes that it will not prosecute, prosecute, or punish the person whose extradition is sought for a crime before extradition other than the crime or the crimes that were the subject of the extradition request, and it also undertakes to prosecute him for a fair trial and to ensure that he is subject to a fair trial.

2. Procedures of the country from which extradition is requested:

According to the provisions of international laws, the procedures that the state undertakes if a person is requested to surrender a person is divided into three stages:

The first stage

It consists of receiving the request, taking investigation procedures, collecting inferences, investigating and arresting the wanted person.

The second stage

It consists in interrogating the arrested person and remanding him in custody, or releasing him with or without bail, or preventing him from travelling until the application received by his surrender is decided upon .[27]

The third stage

It is the examination of the request by the competent court and a decision on it by acceptance or rejection, and the court, in the process of that, verifies the availability of the formal conditions that must be followed by the requesting state, as the existence of the extradition file and that it contains all the documents required to be attached to the document. Ensure that the substantive conditions are met, such as the condition of double criminality, or that the public lawsuit or the penalty have not lapsed. As well as making sure that there is no one of the barriers to delivery stipulated, and if it is assured of the availability of the substantive and formal conditions, it requires the surrender of the person subject of the request by a decision issued by it that includes the nature of the offence. After that, the government, which was granted by law, has the discretionary power to surrender the person or not, unless there is a text in its domestic law obliging it to surrender or if there is a text in an international treaty in which it is a party to surrender it, or if there is a text in an international treaty in which it is a party to surrender it. The court that the legal conditions are not available (or that the evidence contained in the extradition request or investigations is insufficient to prove the crime attributed to the wanted person, it may reject the request, and in all cases, the decisions of the court ruling are final.[28]

Among the international agreements regarding the extradition of accused persons, the Convention on the extradition of accused persons and the accused and the judicial assistance parties concluded in 1953, the Greek agreement on the extradition of accused persons in 1986 and the agreement concluded in Hungary in 1988 relating to the extradition of accused persons and judicial assistance The imprisoned convicts and the extradition of the accused in Poland in 1992. In the opinion of the researcher, supported by the researcher, believes that these agreements can be applied in the field of cybercrime, so that member states may request the extradition of a criminal from the other country that is a member of the convention to prosecute him or execute the penalty against him (for one of the perpetrators).

However, there is another opinion that thinks that these mechanisms of cooperation between countries are not because not all countries are bound to these agreements, and their implementation may be hit by effective obstacles, the crime whose perpetrators are required to be brought in for prosecution may be political or of a political nature.

Fourth - the system of extradition of accused in the field of cybercrimes[29]

It has already been said that cybercrime is a cross-border crime, so the existing borders between countries no longer constitute an obstacle to the commission of this type of crime, just as the criminal activity is no longer limited to a specific region, but rather extends to a criminal offence. And the execution is carried out in another country, and the impact of that crime extends to other countries and he flees to a country that was not affected by this effect. The criminal can move between a group of countries as he pleases, and it is possible for this fugitive criminal to commit other crimes

in multiple countries, and to escape from justice and the cybercriminal to become an international criminal.

Whereas state agencies work for the implementation of the law and seek to pursue criminals for that purpose, but each state cannot override its borders or cross the borders of another state to practice criminal procedures against regional criminals. For this reason, states needed to resort to solving these forms by establishing a system for the extradition of criminals that would make it easier for the authorities of the attacked state to enforce the law and arrest criminals and return them to the country in which they executed the crime and the trial of the crime. Therefore, most countries have been keen to enact legislation on extradition, in addition to concluding regional and international agreements on extradition of the accused.

Among the most prominent conventions that dealt with crimes of electronic piracy but can be considered as the only agreement which provided for this type of crime, the Budapest Convention on combating IT crimes concluded in the Hungarian capital, Budapest, and known as the International Convention against crimes through the Internet, where he coined the present Convention a large number of From legal experts in Europe and other countries (), which were previously mentioned in the previous requirement. For this, states must strengthen extradition procedures through the effective application of the rule of "surrender or prosecution," which imposes an obligation on the state in whose territory the accused is present, to search and investigate the identity of the criminal inside and his whereabouts, and the whereabouts of the offender and their whereabouts. When it comes to handing it over to another country, the countries of the world must also commit themselves to regulate international law and reconcile the necessities of international judicial cooperation with the requirements of sovereignty to protect against cyberpiracy crimes. The researcher believes that the extradition system, especially in electronic and cybercrime, is the best and necessary solution to take in the matter of combating cybercrimes and the losses resulting from that crime for the public and private institutions, so what is the benefit for the crimes to be set against the crime of public and private institutions. . Extradition is an essential means of reducing cybercrime.

Fifth requirement

International cooperation in the field of training to reduce cybercrime and its importance

Training is a continuous and planned activity aimed at bridging the gap between the current performance and the expected performance of the incumbent, and then bringing about changes in the behaviour and abilities of the individual or group responsible for performing this job. Training in the security field has also been defined as preparing security men or law enforcement authorities and training them to confront crimes to provide them with sufficient expertise and skills to confront crimes.

Training is part of the administrative development process, as it is concerned with efficiency and effectiveness in the achievement of work,

and accordingly, many public and private institutions have been keen to pay attention to it as one of the basic tools to raise the level of performance. And the tasks entrusted to them in the best manner. In addition to that, preparing workers to assume more responsibilities by increasing their capabilities to face complex tasks in the present and the future. For this has become seen training as a means of investment employed by administrative organizations to achieve its objectives as a vital element necessary for the building of expertise and skills of renewable fact that training has become an important role in human life in the present era, has increased interest in training in various technical aspects, and has become a necessity for everyone The trainee and the organization to which he belongs at the same time.

The importance of training is represented in the fact that it is the actual and applied method of successful and effective action that ensures they benefit from the skills and experiences of others through competent persons who are qualified and can transfer these experiences and possess these skills using effective means. On the errors and negatives that can reveal the practical application of laws, regulations and regulations, and the development of solutions to avoid them. Accordingly, training has a very important and effective role in combating cybercrime, and we will explain its importance, methods and role in combating those crimes. The operational reality has proven that there are crimes related to the computer and the Internet that have been committed in front of the watch and hear of the policemen. Rather, the policemen extended a helping hand to the perpetrators of these crimes, unintentionally and out of ignorance, or based on the perpetrators of these crimes. This is what happened when one of the police departments in the United States of America asked a company that had been subjected to piracy to stop operating its automated device to be able to put it under surveillance to uncover the perpetrator of the crime and the result of that was the destruction of the file. The emergence of these new patterns of crimes has led to a heavy burden on all criminal justice agencies, whether judicial officers, investigation personnel, or courts of various degrees. Especially since the requirements of justice require that the government security agencies bear full responsibility towards discovering all information crimes to arrest the perpetrators .[30]

For this reason, these devices of all kinds needed to be of a great degree of competence and knowledge and the ability to uncover the ambiguity of those crimes and identify the perpetrators with infinite speed and accuracy. This will not be achieved except through training. The efficiency of the men of justice to confront these new phenomena and their ability to address them must be based on how to develop the training process and upgrade it and advance the methods of achieving its objectives, and from this standpoint, the case was based on the necessity of preparing the training process. As no country can confront these new patterns on its own without the presence of cooperation and coordination with other countries, international coordination and cooperation needed to take place in the field of training judicial officers.[31]

Training here is not intended as traditional training. It is not sufficient for criminal justice men to have the legal background or the elements of police work, but rather they must have technical experience in the field of informational crime. This technical expertise does not come without specialized training in which the personal elements of the trainee are taken into account in terms of scientific suitability and the mental and psychological abilities to receive training, so it is easy to train specialists in information technology and the communications network, rather than training personnel. Some experts argue that the trainee should have an experience of no less than five years in areas related to information technology, such as programming, system design and analysis, network management and operations computer.[32]

Conclusions

1. Existence of cooperation between police agencies in various countries, the most prominent of which is the establishment of the International Criminal Police Organization (INTERPOL) to combat cross-border crimes, including the implementation of cybercrime, in the same way. And the establishment of the International Web Police and the Internet Fraud Report Center to receive reports and track the crimes and fraud that are committed through the Internet.
2. The role of the international community in confronting those crimes through international judicial cooperation through the exchange of information and documents required by foreign judicial authorities in connection with one of the crimes, as well as the transfer of procedures for the conduct of criminal offences, as well as the transfer of procedures for such crimes. Another, and activating the judicial delegation that enables one country to benefit from the public authorities in another country if the regional borders prevent it from enforcing its law towards the criminal.
3. The international community has also sought to conclude international conventions to combat cybercrimes, through the conclusion of a treaty in Budapest to combat cybercrime, which is the first of the treaties related to combating those crimes.
4. Also, the existence of a system such as the system of extradition of the accused had a significant impact on demonstrating the role of the international community in confronting cybercrime and its cross-border privacy.
5. The international cooperation has also emerged in the field of combating cybercrime by holding international training courses for the national agencies of the countries charged with dealing with those crimes at the national level and to reach an important result, which is that the advanced countries can help you without them. On training security authorities in developing countries to confront these crimes.
6. Despite the existence of this tangible international cooperation, difficulties and obstacles are facing this cooperation that limits the effectiveness of the enforcement of cooperation represented.
7. The diversity and difference of legal and procedural systems from one state to another in terms of methods of investigation and investigation and the extent of legality and legality of criminal procedures from one state to another, so what is considered a legitimate procedure in one state may be

considered unlawful. Likewise, the problem of judicial competence may limit this cooperation, as the difference in legislation and legal systems results in a conflict of judicial jurisdiction between countries, which hinders international cooperation.

8. The existence of a condition of double criminality that must be in place. The extradition of the accused is not enforceable is an obstacle to its enforcement because an act may be criminalized in one country without the other, resulting in the inability to extradite the criminal.
9. Likewise, if there is international judicial assistance, but the mechanism for its implementation is through a diplomatic path that is slow and complicated, which conflicts with the nature of cybercrime and the Internet, which is characterized by speed.

Recommendations

1. Work to remove the obstacles of the procedural systems of states and the recognition by states of the penal procedures of other countries as long as these procedures are legitimate in the aggressed state.
2. Work on concluding international agreements in which unifying views between states regarding the issue of judicial jurisdiction disputes about Internet crimes and updating the substantive and procedural criminal laws in proportion to the criminal offences.
3. Reducing the application of the requirement of double criminality, which is one of the most important conditions of the extradition system, by including general provisions in treaties and agreements on extradition, and that is by specifying any acts that must be criminalized or criminalized. Of the penalty in each country.
4. About the difficulties related to international judicial aid and the slow response, we find an urgent need to find a speedy way in submitting requests for representation, such as allowing direct contact with the competent authority to look into these requests to adjudicate the issue of extradition.

References

1. Amir Faraj Youssef, Cyber and Informational Crime and International and Domestic Efforts to Combat Computer and Internet Crimes, Al-Wafa Legal Library, 2011 ed.

2. Jamil Abdul Baqi Al-Sagheer, Procedural Aspects of Internet-Related Crimes, Dar Al-Nahda Al-Arabiya, 2001 Edition

3. Hussein bin Saeed Al-Ghafri, Criminal Policy in the Face of Internet Crimes, Dar Al-Nahda Al-Arabiya 2009.

4. Hassanein Saleh Obeid, International Criminal Law, Its History - Applications - Its Projects, Arab Renaissance House, Cairo, 1977 Edition.

5. Hussein bin Saeed Al-Ghafri, International Efforts to Confront Internet Crimes, Dar Al-Nahda Al-Arabiya, 2009.

6. Khaled Tohme Saafak Al-Shammari, International Criminal Law, Noor Charitable Library, Kuwait, Second Edition, 2005.

7. Suleiman Ahmed Fadl, The Legislative and Security Confrontation for Crimes Arising from the Use of the International Information Network, Dar Al-Nahda Al-Arabiya, 2007 Edition, Egypt.

8. Suleiman Abdel-Moneim Suleiman, problematic aspects of the legal system for extradition, University Publications House, 2015 edition.

9. Omar Muhammad Bin Yunus, European Convention on Virtual Crime, without a publisher, 2005.

10. Ghanim Mardi Al-Shamir, Information Crimes (what they are - their characteristics - how to deal with them legally), House of Culture, Jordan, 2016 edition.

11. Fahd Abdullah Al-Obaid Al-Azmi, Information Criminal Procedures, New University House, 2016 Edition, Egypt.

12. Munir Muhammad Al-Juhani, Mamdouh Muhammad Al-Juhani, Internet and computer crimes and their means of combating them, Arab Thought House, Alexandria, 2004 edition.

13. Medhat Ramadan, Crimes of Assaults on Persons and the Internet, Dar Al-Nahda Al-Arabiya, Edition 2000.

14. Muhammad Al-Sayed Arafa, Training for Men of Justice and its Impact on Achieving Justice, Naif Arab University for Security Sciences, Riyadh, 2005.

15. Hilali Abdullah Ahmad, The substantive and procedural aspects of information crimes (in light of the Budapest Agreement 2001) Dar Al-Nahda Al-Arabiya, 2001 Edition.

16. Youssef Hassan Youssef, International Internet Crimes, The National Center for Legal Publications, Cairo, First Edition, 2011.

17. Sidqi Al-Rahim, International Cooperation in Contemporary Thought, Journal of Law and Economics, Cairo University, 1983.

18. Souad Boukhafeh, The Principle of Extradition and Trial in Light of the Work of the International Law Commission, Master's Thesis, Faculty of Law, Ben Aknoun University, Algeria, 2014.

19. Samar Khadr Saleh Al-Khodari, Extradition Provisions for the Accused in Palestine, Master's Thesis in Public Law, Faculty of Law, Al-Azhar University, 2010.

20. Salem Muhammad Suleiman al-Anjuli, Provisions of Criminal Responsibility for International Crimes in National Legislations, PhD's thesis, Faculty of Law, Ain Shams University, 1997.

21. Saleh Muhammad Al-Nuwaijim, Evaluation of the Efficiency of the Training Process in Security Training Institutes in the City of Riyadh from the Point of View of Their Employees, Master's Thesis in Administrative Sciences, Naif Arab University for Security Sciences, Riyadh, 2005.

22. Alaa El-Din Shehata, International Cooperation in Combating Crime, without a publisher, Cairo, 2000 Edition.

23. Issa Salim Daoud, Electronic Piracy Crimes, Master Thesis, Alexandria University, 2017.

24. Amr Zaki Abd Al-Mualla, The International Treaty to Resist Computer Crime, a working paper presented to the Conference on Legal Aspects of Electronic Commerce, the League of Arab States Headquarters, January 2001.

25. Hammar Fafa, Extradition Procedures for Accused in Algerian Legislation in Light of International Agreements, Master's Letter, Faculty of Law and Political Science, University of Oran, Algeria, 2014.

26. Al-Quotas Magazine, published by the Judicial Institute of the Republic of Sudan, Tenth Edition, September 2003.

27. Mabb bin Abdullah Al-Sanad, International Cooperation in Executing Criminal Judgments and Its Impact on Achieving Justice, Master's Thesis, College of Higher Studies, Naif Arab University for Security Sciences, Riyadh, 2011.

28. Hisham Muhammad Farid Resam, Information Crimes, the Principles of the Technical Criminal Investigation, a paper presented to the Conference on Law, Computer and the Internet, College of Sharia and Law at the United Arab Emirates University, from 1/5/2000, Volume Two, Third Edition.

29. Yasser Muhammad al-Jabour, extradition or presentation of the accused in international conventions and the statute of the International Criminal Court, Master's thesis, College of Law, Middle East University, Amman 2011.

30. http://usinfo.state.gov/iournals/itgic/0801/ijga/art3.htm Web Police site.
31. http://www.web-police.org Website of the Internet Fraud Report Center.
32. http://www.un.org/arabic/documents/instruments/docs_subj_ar.asp?subj=33 Transliteration Arabic References.