DOI: 10.33193/JEAHS.5.2021.169

ISSN Online: 2709-071X
ISSN Print: 2709-0701

مجلة العلوم التربوية والإنسانية
Journal of Educational and Human Sciences
www.jeahs.com
Volume (5) April 2021
العدد (5) أبريل 2021

Investigating Electronic Defamation Using The Internet

Nibras Salim khudhair
Law Department - Al Kunooze University College
Basra, Iraq
Email: nibras.s@kunoozu.edu.iq

ABSTRACT

The study was aimed at identifying the most important methods that help in developing criminal investigation skills to confront cyber-crimes. The study was based on more than one approach. It was based on the inductive method, which is based on the deductive approach. The most important findings were: Electronic evidence has a specific scientific value in referring to the facts it contains, but it is indispensable that it be legitimate, both in terms of existence, to be among the legally accepted evidence as a means of proof. 1. The reasons for the difficulty of detecting cybercrime can be explained by the fact that this crime does not leave any visible external impact that the offender can commit this crime in other countries and continents because cybercrime is a transnational crime. 2. The lack of technical and technical expertise in the police, prosecutors, and the judiciary. This is a major obstacle to proving cybercrime. This type of crime requires training and qualification in information technology, evidence collection, research, and trial in the computer and Internet environment. 3. Cybercrime may be part of traditional crime, in the sense that there is a traditional crime involving an electronic aspect.

Keywords: Investigating, Electronic, Defamation, Internet.

Introduction

In the light of today's scientific, technological, and information revolution; all countries are racing to acquire this technology and exploit its amazing potential in all fields. Most developing countries are trying to import and transfer modern and widely diffused technology **(Hindi & Rifai, 2017)**. Information technology has become an essential component of the economic development and backbone of knowledge-based economies in terms of operations, quality of service delivery and service productivity. The use of information technology is therefore an increasing challenge for developing countries. There is now growing evidence that knowledge-based innovation is a critical factor in the competitiveness of countries, industries, organizations and companies. Institutions like the banking sector have benefited greatly from e-banking, an IT application to enhance competitiveness **(Oluwatolani et al., 2011)**.

The Internet market has grown exponentially, and online purchases and sub-prime banks have seen this growth. Many companies were quick to identify different ways to exploit them as required. By making a huge online product it is almost inexhaustible and puts the Internet at the top of the list of convenience. In this rapidly evolving modern society, of which we have all become part, comfort has become necessary to escape the ever-increasing pace of life. In particular, e-business, an IT application that has the greatest impact on the global economy, is creating a new business environment **(Adetayo et al.1999)**. The Internet is widely spread all over the world and has become an integral part of information technology within companies as well as many homes **(Akpore, 1998).**

Crime is defined as an illegal act punishable by a state or force, and the number of cybercrime is increasing rapidly because technology is growing very rapidly. The investigation of cybercrime has become a very complex task to be undertaken without an appropriate framework. There are a wide range of different types of Internet crimes today and the Internet is the fastest infrastructure in everyday life. The user can send and receive any form of data. The scope of electronic security is not limited to the security of the information technology industry but also to cyberspace. Internet criminals have become more sophisticated and target consumers as well as public and private institutions. All types of cybercrime consist of both the computer and the person behind it as victims. Electronic crime can include anything like downloading. Many countries and governments now impose strict laws on electronic securities in order to prevent the loss of some important information **(Kaur, 2018)**, And technology crimes relate to the word technology that includes the computer network, so anyone who can use to do any activity in the world in real time. Cybercrime such as fraud, child pornography, intellectual property, identity theft or privacy violation are used by digital data from computer systems and other electronic devices **(Dacey & Gallant,1997)**.

For the majority of people, the Internet is still vague, forbidden, incomprehensible and frightening. Along with the explosive growth of the Internet has led to the growth of cyber-crime opportunities. As a result of the rapid adoption of the Internet worldwide, computer crimes include not only piracy and cracking, but also extortion, child pornography, money laundering, fraud, software piracy and corporate espionage **(Choi et al., 2007)**.

These devices are used as a target by attacking the computer through viruses, as a weapon to commit crimes, or as a supplement to store illegal information. Internet crime also affects businesses every year, losing billions of dollars and damaging the company's reputation, leading to future business losses as well. In today's world, electronic systems provide flexibility that leads to their illegal use. With the government's Internet-framed policy, the Internet along with facilitating economic activities such as buying, selling, online transactions and social networking brings many threats. Piracy tools are available on the Internet that do not require people to be highly skilled and encourage them to do inappropriate work online. Thus, cyberspace may make users vulnerable, making it important to take the necessary steps and avoid exposure from verbs. High-population countries such as Asia rely on web resources that create an opportunity to commit such crimes, and make it difficult to detect and prevent cybercrime in a WAN environment **(Choi et al., 2007)**. Law enforcement officials were frustrated by the inability of lawmakers to keep cybercrime legislation ahead of the fast-moving technological curve. At the same time, legislators face the need to balance competing interests **(Jain & Shrivastava, 2014)**.

The criminal investigation and the collection of conclusions from the security activities that top the attempts to confront the crimes developed through the development of methods and improve the investigators and provide them with modern science and technology. The scientific and technical development of the countries in general and the criminal investigation in particular have helped this technological and digital revolution and the provision of advanced equipment and modern communication systems, but even to include new ways in working to extract the truth from the clutches of fainting to find the right path, and this will be achieved only through familiarity In terms of technical and criminal research, in accordance with advanced technology, especially in crimes that are described as new patterns of the relationship between the methods of committing modern science and technology, such as organized crime, high-tech crimes, money laundering, Civil aviation disaster **(Al-Balawi, 2009)**.

Study Problem

Each era has its own characteristics and functions. The current era is marked by the advent of the world's ICT revolution and the consequent change in the lifestyle of individuals and governments. It is a recognized fact that technological progress has an impact. Law and reality in the context of progress, the law must not be separated from the reality that results from and applies to it, but must be responsive and developed at the same pace of development **(Jamal, 2018)**. Recently, modern technological development has produced a complex pattern of crimes committed by skilled criminals in the means of committing crimes technically and accurately. The offender sought to use technology to pass his crimes on the police. The police also sought to obtain the latest technology to invest in crime detection, especially since there is now known as the complete crime where the theories and scientific research are necessary in this regard, it is basic to leave the criminal some of the effects in the crime scene and vice versa to leave the scene of the effects of crime on the offender and this is the thread that reaches the solution of this crime is the failure of the security services to access the culprit, as well as the failure of the security services to obtain the latest techniques that reveal what is unknown by analyzing the physical and biological effects. The human element must therefore be trained in techniques to keep abreast of the latest developments in this area **(Al-Balawi, 2009)**. Complicating the enforcement of cybercrime is the area of legal jurisdiction. Such as legislation to combat such crimes, no single State could effectively enact laws that comprehensively addressed the problem of Internet crime without the cooperation of other States. Law enforcement agencies around the world are working together to develop new partnerships and new methodologies to reduce cybercrime in order to ensure safety and security on the Internet. Given their global dimensions and unlimited nature, new and innovative responses are needed for the cause of cybercrime or computer crime in general **(Jain & Shrivastava, 2014)**.

Study Questions

Through the problem of the study has developed several questions, the most important of which are the following:

1. To what extent are criminal investigation skills available to investigators in the Commission on the Investigation and Prosecution of Cybercrime?
2. What are the main obstacles to development that prevent the development and mastering of criminal investigation skills in cybercrime?
3. What are the most important methods and methods that help in developing criminal investigation skills in the face of cybercrime?
4. What are the implications of society through electronic defamation?

Objectives of the Study

This study aims at identifying the most important methods that help in developing criminal investigation skills to confront cyber-crimes by achieving the following objectives:

1. Determine the criminal investigation skills of the investigators in the Commission of Inquiry and Prosecution of Electronic Crimes.
2. Identify the most important obstacles to development that prevent the development and mastering of criminal investigation skills in cybercrime.
3. Identify the most important methods and methods that help in developing criminal investigation skills in the face of cybercrime.
4. Identify the effects of society through electronic defamation.

The first part: Fundamentals of Information Technology

The history of information technology is the history of the information itself, because man in the early stages of communication with others and nature felt something today known as modernization, used tools to express himself. In fact, the beginning was just a simple signal moving individuals in prehistoric society through movements. The simple tools that existed at the time to become in a complex form of media channels and advanced means of communication and their rules and contents and information banks are derived from hardware and software. The information technology began with the emergence of information from the use of signals and the storage, preservation, recording and writing of information on wood, stones, skin, clay and papyrus were evidence of multiple inventions for one purpose. Thus, the successive inventions and the revolution brought by Gutenberg in Germany the second half of the fifteenth century, then the printing of animated characters, considered by some as the first information revolution. Then the industrial revolution in Europe, as well as the development of scientific research and the growing importance of information in all aspects of human life played a prominent role. In the second half of the 20th century, there were many rapid developments in information technology, from the invention of computers and their accessories to the use of networks and information systems to become electronic information, where people can contact anyone anywhere in the world. Just enough to provide a computer and a network can know the world through the push of a button, making the world a small community. But that information technology generated a generation of skilled, where the circumvention of the use of these means, for example, prefer to communicate through the program provided by Skype better than using a mobile phone **(Tommy, 2006)**.

1. The concept of information technology and related concepts:

1.1. The concept of technology:

The term "technology" generally refers to the means and devices used by man to guide life affairs. The "technology" is the search for the best available means, exchanging and facilitating the quick and effective access to its applicants. This reform has gained importance from its close relationship with the openness of knowledge and the information revolution. Its main role in achieving the goals of the libraries and each of the information centers and sources of learning in facilitating the availability and access to information accurately and quickly to the public of beneficiaries Especially those with disabilities, provide opportunities to meet their needs to the same extent as opportunities for groups of beneficiaries without disabilities **(Ali, 2016)**.

The concept of technology is one of the concepts discussed by many researchers and thinkers, and they differed in their view because of their different specialization and the development of the characteristics of the technology itself, but it is agreed that technology is as old as human inventions. And then became a tool used to serve him and help him to meet the growing needs, and then developed and used to the extent that became very important in his public and private life. Making some thinkers responsible for most of the changes taking place within contemporary society **(Delio, 2010)**.

1.2. Information technology:

Many researchers have sought to develop a brief definition of information technology. In recognition of the breadth of materials and concepts proposed by the term "mass", information technology has been used to represent convergences of communication, video and computing technology, or rather technologies that support application diversity in microcomputer and video, multimedia, the Internet, the World Wide Web, etc.) **(Williams, n.d.)**.

IT has been defined as computer programs and solutions that provide support to management, operations and strategists in organizations **(Thong & Yap, 1995)**.

Attaran **(2003)** defines IT as the capacity provided to organizations through computers, software applications, and telecommunications to provide data, information and knowledge to individuals and processes.

Information technology can be defined as recently mentioned Tan et al. **(2009)** as an application of ICT tools including computer network, software and hardware required for Internet connectivity. Based on this review and its alignment with the above-mentioned views, MTR will cover a wide range of information processing and computer applications in enterprises. It includes information systems, the Internet, information and communication technology, and their infrastructure, including computer programs, networks and devices, that process or transmit information to enhance the effectiveness of individuals and organizations. However, IT also includes any computer application, hardware packages, computer-aided manufacturing, computer-aided design, electronic data interchange and ERP that positively affect collaboration productivity.

There are different definitions of technology; the technology is divided into four elements as follows, as Beig et al. **(2012)**:

A. Technical tools: Device includes technology.

B. Human Tool: A group of people who participate in the production system.

C. Tools or documentation Information: Documents that identify and describe technology

D. Regulatory tools: an atmosphere in which these three components can be coordinated and conducted. Each technology incorporated these four components.

2. Benefits of Information technology:

The role of information technology is now very clear. Every day more companies invest in information technology to achieve competitive advantages that make them more realistic. Many companies are pushing for investments in information technology. These investments are now concentrated not only in hardware but increasingly in systems the information. He became aware of the administrative support provided by these systems as well as the benefits of their use **(Bushati et al., 2015)**.

3. Advantages and disadvantages of Information technology:

The main advantages and disadvantages of information technology are as follows:

3.1. Information technology features:

One of the most important features of information technology is the following:

A. Globalization: Globalization is one of the major phenomena of this age, and its scope is very broad and multi-influence affects factors such as economy, politics, culture, lifestyle, and especially science and technological advances. The process of globalization is said to include the evolution of information technology, characterized by advances in electronics, computers and telecommunications, made possible through scientific and technological breakthroughs in the reduction of integrated circuits, transistors and semiconductors. Emerging technologies play a vital role in enabling the globalization of economic and social activities to flourish. It is right to say that the era of globalization has brought about the rapid proliferation of computers and the use of the Internet, satellite and mobile phone in the world, particularly in Nigeria where communication has been difficult and communications facilities are inadequate in our main urban, semi-urban and rural areas. At present, with the introduction of mobile phones, many rural areas now have access to communication facilities and communicate seamlessly with the rest of the world **(Murtala, 2005)**.

B. Communications: Communication is now one of the most important assets in organizations. This is because organizations can not only be considered as "containers" for individuals with common objectives, but they must be considered sophisticated social contexts in which real people face different situations and problems. Communication is therefore the means to understand and adapt to the dynamics of these changing environments **(Cuel and Ferrario, 2006)**, With the help of IT, communication becomes cheaper, faster and more efficient. We can now communicate with anyone around the world simply by sending them text messages or sending them an almost instant response email. The Internet has also opened face-to-face direct communications from around the world through video conferencing assistance **(Kumar, 2014)**.

C. Cost-effectiveness: Over the past few decades, modern businesses have been investing increasing amounts in information technology to improve their operational efficiency and competitiveness in the industry. The important role that IT plays in contemporary business is beyond doubt. Information technology is a critical factor for businesses to survive and grow further; however, empirical evidence supporting these expected benefits has been mixed. Some researchers emphasized that IT investments can actually enhance the operational performance of enterprises by reducing costs, increasing profit margins, raising production levels, increasing service quality, enhancing customer satisfaction, and improving overall processes. In contrast, other researchers have not demonstrated the positive impact of IT investments and have concluded that IT spending has made no significant contributions to corporate operations. Thus, the "discrepancy in IT productivity" has been the subject of decades of debate **(Li, 2007)** .

D. Bridging the cultural gap: Over the last decade there has been increasing interest in the impact of cultural differences on the development and use of ICTs. The world continues to move towards world markets through interactions among members of different cultures. In fact, global activities are greatly facilitated and supported by current ICTs. It is therefore important to understand the impact of cultural differences on these activities with the widespread spread of information technology (IT) on a global level, it is increasingly possible to witness the same technology used in many different cultures **(Yeganeh, 2002)**.

E. More time: Information technology represented by the Internet recently made it a way to recognize, use, manage and organize time, although it is generally accepted that information technology affects the temporal aspects of contemporary society, but the relationship between time and information technology often fails to recognize the complexity of their relationship They are simply understood in terms of formalities. The effect of technology on time is that many things are getting faster, it is believed that the associated changes are more important than the time itself **(Lee and Whitley, 2002)**.

F. Create new jobs: Perhaps the best advantage of IT is creating new and interesting jobs. Computer programmers, system analysts, hardware and software developers and web designers are just some of the many new job opportunities created with the help of IT **(Kumar, 2014)**.

G.

3.2. Disadvantages of information technology:

One of the main disadvantages of information technology is the following:

A. Unemployment: Although IT has contributed to streamlining the business process, it has also created additional jobs, downsizing, and outsourcing. This means that many low- and middle-level jobs have been eliminated, making more people unemployed **(Kumar, 2014)**.

B. Privacy: ICT is one of the fastest growing sectors, and the importance of ICT cannot be ignored because it affects all aspects of society, including telecommunications, education, banking, trade and employment. However, the issue of individual privacy in this sector is a particular challenge as individuals disclose greater amounts of personal information than ever before at a time when there are no specific laws or regulations **(Almatarneh, 2011)**.

C. Lack of job security: Industry experts believe that the Internet has made job security a big issue as technology continues to change with every day. This means that one has to be in continuous learning mode, if he wishes to have his job safe **(Kumar, 2014)**.

D. The dominant culture: Although technology facilitates daily life, it has many obstacles. It is important to look at culture and culture trauma from the perspective of the digital age. Cultural shock and culture seem to have new aspects because of its technology and facilities. Today, it is normal to see or live the cultural advantages of the home in front of television or the Internet or with other techniques by other members of culture. There are used for physical barriers and cross-border in order to interact with a different culture. However, today one does not need to leave the comfort of his or her own environment to be exposed to alien cultures. Technology has already removed physical barriers and boundaries between cultures. People are exposed to different cultures on a daily basis because of TV shows and the Internet. They quickly accept and adapt various cultural practices. If people understand the cultural similarities between societies, re-adaptation and re-adjustment will not be as difficult as before. Before recognizing physical barriers, he / she can prepare himself, mentally or psychologically for cultural situations. The problems faced by other countries can be solved by eliminating mental barriers, to be more descriptive and illustrative **(Kurt and Gök, 2015)**.

The second part: Electronic Crimes in Public International Law:

The crime resulting from the misappropriation of the IT revolution is entirely different from conventional crime in nature, content, scope, effects, types, methods and tools, and is specific to the perpetrators. Rapid urbanization, the desire for wealth, the availability of opportunities for proliferation, the high proportion of victims, particularly with the lack of controls, weak legal legislation and the imposition of penalties for curbing the effects of such crimes against individuals, statements and States, Different sectors, they represent the reality of electronic colonization in its worst forms **(Bounaara, N.D.)**, Cybercrime is one of the most serious security challenges facing all the world's communities in the use of ICTs across the public, private and private sectors. Computer crimes are means of committing fraud, stealing identity cards, credit cards, financial balances, forgery, embezzlement, theft of intellectual property rights, vibration, behavior and sexual exploitation of children, as well as the promotion of extremist ideas and the support and financing of terrorism **(Research and Studies Complex, 2016)**.

1. The concept of cybercrime:

The crime means that a person is actually committing a criminal offense and is punished for it, or refrains from doing an act that enjoins the Shari'a to punish him and prepares to leave him punished. This is because Allah has decided to punish any person who violates his commands and intentions, and is executed by God. Every crime in the Sharia has an urgent punishment in this world **(Boulmain,2008)**, The crime is defined as a negative social phenomenon that expresses the confusion and imbalance in social relations and social behavior and embodies the nature of the contradictions in the subjective and subjective variables that affect the human environment and the social life and characterizes the nature of the human problems suffered by the individual and society alike **(Hassan,1993)**, As for the crime from the legal point of view, it is any act that is contrary to the provisions of the Penal Code. It is an immoral act that alienates the souls **(Arim, 1970)**.

There were many views on the concept of cybercrime according to the corner view that constitutes cybercrime. Some studies tend to be defined in the light of the adoption of a methodology based on classification of computer-related activities for categories and species and for each type of specific cognition of the crime associated with them **(Attai, 2015)**, After identifying the concept of crime, it is necessary to identify the concept of the main subject, namely, the concept of electronic crime, and

the most important definitions that I have defined as follows:
Define cybercrime in short as crimes committed using computers, networks and technical equipment **(Badia, 2014)**, The crime is all that is prescribed by the law or the law to criminalize the acts and words and to make it an explicit punishment, such as border crimes and punishment or granting the judge the power to determine the penalty, as in many crimes, and therefore the act is not a crime except when there is a provision, Of the application. The human being lives in a society of people, and its effectiveness, which is manifested in the assertion of its natural rights and its use, can only be exercised within the limits of the laws and to the extent that its growth is not detrimental to the growth of the effectiveness of other people. Those who exceed these limits are concerned about the social system. The situation is the punishment provided for in the Penal Code **(Marquezia,1983)**.

2. Electronic defamation:

The most important development in the world today is the technological revolution, especially the communications revolution, the communication revolution is the main engine in the current developments. However, it is not the only engine in these developments. The great development of computer technology has greatly contributed to accelerating progress in the field of communications and information. The emergence of tools, inventions and new services in various fields has been a product of the development of both sides. The technological revolution has led to the emergence of a new type of transaction called electronic transactions that differ from the traditional transactions we know, in terms of the environment in which these transactions occur. Electronic transactions are all transactions made through electronic equipment such as telephones, faxes, computers, the Internet, and recently via mobile phones **(Hijazi, 2005)**, And the types of crimes represented in electronic defamation:

2.1. Communications in the promotion of criminal plots:

This includes organized criminal activities promoted or facilitated by technology, such as arms smuggling, money laundering, drug trafficking, gambling, prostitution and child pornography. Criminal networks have been discovered that extend across national borders, operate with a high degree of coordination and use sophisticated methods of concealment **(Longe et al., 2009)**.

2.2. Dissemination of offensive material:

There is content that some people consider highly objectionable in cyberspace. This includes, inter alia, sexually explicit material, racist propaganda, and instructions for the manufacture of inflammatory and explosive devices. Communication systems can also be used to harass, threaten or enter invasive communications, from the traditional obscene telephone call to their contemporary appearance in "electronic prosecution", where persistent messages are sent to an unwanted recipient. In one case, it was alleged that a man stole naked pictures of his former girlfriend and new boyfriend and posted them on the Internet with her name, address and telephone number. The unfortunate couple received phone calls and e-mails from strangers like Denmark who said they saw the pictures online. Investigations also revealed that the victim kept records of women's movements and collected information about her family. Computer networks can also be used to promote extortion. In England, financial institutions reportedly paid large sums to sophisticated computer criminals who threatened to destroy computer systems **(https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime)**.

2.3. Cyber sabotage, terrorism and extortion:

There have been recent cases of extortion that threaten the security and safety of society, a form of modern cybercrime, and look through the social networking sites used by some to overcome young girls, as well as hunting by some young people or specialized gangs outside the state and their contributions to hunt young people to raise funds in malicious ways through the exploitation of girls who play the role of love and inspiration for young people. The majority of girls were blackmailed by men who seek to establish illegal relationships or expose girls by showing their images in inappropriate situations. In social networking sites, which made these girls live harsh humanitarian conditions with their families, and confirmed the police and the prosecution that many cases of extortion did not reach the police stations for fear of scandal **(Al-Alfi,N.D.)**.

2.4. Fraud in sales and investment:

Despite the recurrence of these crimes in light of the increasing number of Internet users and the increasing volume of e-commerce, there is still much uncertainty about how to deal with these crimes, and there is also much controversy about the traditional concept of commercial fraud and its applicability to cybercrime. Fraud is defined as any act that would alter the nature or characteristics of the material or its usefulness to which the actor has entered. It is also known as any intentional act that the commodity has a change in its characteristics, characteristics or intrinsic characteristics, and generally, the elements involved in its composition, so that the other is deceived. It is easy to identify fraud in cases of a physical or visual nature, such as selling rotten meat, selling toxic drugs, mixing kerosene gasoline, selling auto parts and counterfeit machines, selling cosmetics and expired face powders. But in cases of cyber-crime, that physical or visual nature may not be readily available **(Hijazi, 2004)**.

2.5. Fraud in the transfer of electronic funds:

Fraud in information about e-money systems is one of the most important cases of fraud in the banking sector. There is a wide variety of forms of fraud, which contribute to the computer to a large extent, including, for example, relying on computers to create fake loan guarantees. The manipulation inside the bank, which is through its computer-assisted staff and perhaps one of the most prominent cases of fraud in this area, is related to bad tools, which are tools that have been accepted by the bank but due to some of its associated shortcomings are rejected by however. Some shortcomings can be that the link is rejected by the central computer **(Abdul-Jabbouri, 2014)**.

3. Characteristics of the cyber-criminal:

The criminal is a natural person, has the ability to run the computer as a user, not only with the ability to experiment, but also with the ability to commit crime on the computer. Characteristics of the offender are as follows **(Al-Afifi,2013)**:

3.1. The cyber-criminal is a social person:

The criminal is a unique category in the world of criminality, because this criminal is a nonviolent person, unlike traditional criminals. He has a sharp intelligence that helps him adapt to the members of the community. He is worried and puzzled. He commits his crime quietly, recounts it and obliterates its effects easily. This moment is a natural person, and at another moment a professional criminal. Much of what drives the offender to commit his crime is revenge from the employer who fired him from his job, or to show his ability to penetrate members and sites, or motivated by amusement, monument or physical motivation. Because cybercriminals are socially adaptable, there are those who believe that the more dangerous they are, the greater their ability to adapt to society. Cybercriminals often go back to commit their crimes again. It is prohibited to return to criminality, in order to challenge the gaps that led to its submission to the Court in the first place. The return of the offender may be brought to trial again. The cyber-criminal has nothing to do with the crimes. Often, Internet crimes are committed alone.

3.2. Electronic criminal Smart and specialized criminal:

One of the most important characteristics of an electronic criminal is that he is an intelligent criminal. We do not find this intelligence in the traditional criminals who often have an impact on them. Unlike the electronic criminal, he has suffered all the technical and technical aspects of his crime, which helps him to get rid of his evidence quickly and effortlessly. This is the case of most of these criminals, but the experience of the cyber-criminal may be limited only in the knowledge of the circumstances of the crime, if the puzzlement of the criminal few, the crimes committed by the damage does not exceed or copy data and programs, but if the offender has a high level of experience, Commits a crime Hacking devices, cybercrime, viruses, or stealing money. In many cases, cybercriminals are specialized criminals, that is to say, they specialize in cybercrime and computer crimes. In their crimes, these criminals may also limit serious crimes.

The third part: Criminal investigation:

There is no doubt that the current evolution of the communications revolution and the results of this revolution from the advanced electronic means and the many have been reflected in the impact of the events that resulted from them, and characterized these crimes in a special way in the means that are committed, and where is located, and the perpetrators presented to those who possess the supernatural intelligence, Between artificial intelligence and human intelligence, making it difficult to confront them criminally. The current development, which had an impact on the Penal Code, had an impact on the Code of Criminal Procedure, so that some of the provisions of the Act had not been applied because the first law could not accommodate emerging crimes committed by electronic means. The current reality after the information revolution does not depend on the adequate legal protection of advanced crime that may not be limited to the scope of the place and cannot be replaced by traditional material objects known to people. May also be committed to innovative means of advanced technology, and see it as concrete material **(Jamal,2018).**

1. The concept of criminal investigation:

It is said that it has achieved any evidence and honesty and is said to have investigated doubts and achieved the statement and the issue and achieved the dress is the most delicate fabric and dye dress, which is a polluted dye, in the language aimed at criminal investigation. Some have learned to investigate the verification, and it is said that a person has achieved an order that means investigating this matter, but any gem, attributes and dimensions or he realizes the matter is stripped of illusion illusions **(Ashour,2010)**, According Nasser **(N.D.)** Criminal Procedure Group The Investigator shall be fully punished as a judge in the crime, provided that he is convicted of a crime, place or time of the offense, whether committed by the perpetrators or by others.

2. Essential elements for achieving informatics crimes:

These elements are as follows **(Tarizi, 2017)**:

2.1. Determining the time and place of committing the informational crime:

The criminal outcome of e-crime raises many problems, for example where and when the criminal outcome of e-crime is achieved. If the accused commits a crime in a country by penetrating a bank account in another country, this raises the problem at the time of the offense in the country of the accused or the timing of the stolen bank, as well as another problem in terms of the crime.

2.2. Demonstrating the material aspect of informational crime:

Physical activity or behavior in cybercrime requires knowledge of the physical conduct committed by the offender to commit the crime of information, through computer processing and downloading of programs. Although preparation is a preparatory act in traditional crimes, viruses and software downloads are offenses in themselves.

2.3. Presentation of the ethical angle of cybercrime:

It refers to the psychological state and the will of the offender, which links the seriousness of the crime and the crime of the offender. Public disclosure of the guarantees necessary to provide justice, not only to bring confidence in the heart of the accused, but must include in itself the protection of the judge to be suspect or to be susceptible to influence, which is increasingly public that things are going normally, the public in the investigation stage of proportionality Limited to the adversaries in the Jordanian case, cinema at the trial stage is absolute, any member of the public may attend the trial.

3. The most important obstacles to proof based on digital evidence in information crimes:

One of the most important obstacles facing criminal investigation is relying on digital evidence in cybercrime **(Al-Qahtani, 2014)**:

3.1. Deficiencies in the identification of the offender through digital evidence:

The crime of informatics about conventional crime is that the first crime is rarely necessary to commit any kind of violence except in rare cases, but it is dealt with through the introduction of false or prohibited information into programs Distorting or altering data or information already stored in the computer, transferring malware or spyware to stored data and information.

3.2. Obstruction of access to the manual:

In some cases, the offender sets up technical obstacles to prevent the detection of his crime and the use of encryption techniques or passwords, in order to prevent information about public circulation and prevent third parties, including control devices, from illegally accessing stored data and information And processed.

3.3. The absence of visible evidence of cybercrime occurring in various electronic processes:

such as e-commerce, e-banking or e-government, is subject to important aspects of automatic data processing. Such as theft, theft, theft, seizure, fraud, forgery or destruction, it may be difficult to prove this because of the moral nature of the place where the crime took place.

3.4. Difficulty in understanding the evidence obtained from cybercrime (electronic means):

Reflecting on the understanding of digital evidence on technical devices and software, as well as on the professionals who publish this digital evidence and the nature of the evidence. The digital manual may be included in technical matters that are not only able to be understood by a specialist who uses his or her artwork to perform his work.

3.5. Problems with the procedure for accepting the digital evidence There is no difficulty in proving cyber-crime:

when it is not possible to obtain sufficient evidence to prove it, but this difficulty extends to the procedure of obtaining this evidence because criminals who commit their crimes by modern electronic means the smart class that strikes a security fence because of their actions, Makes it more difficult for search procedures to search for evidence that may condemn them by using passwords that do not allow others to access data stored electronically or transmitted through such criminals. They may also use hidden instructions between these words or use code or encryption For their special even impossible for others see them.

Funding & Results:

The study found that the authorities' research problem is the legal value of the electronic evidence obtained in the forensic process, in other words, the extent to which the evidence is accepted as evidence from the investigating judge. Traditional or innovative are not as easy as they were, but are often hampered by difficulties related to either the pattern of electronic evidence or to the human factor. The fact that there is evidence that the crime was committed and attributed to a particular person may not be sufficient to justify it. Instead, the manual must have a legal value, based on two basic questions: the first is the legitimacy of the evidence, and the second is justified to prove the facts. Electronic evidence has a specific scientific value in referring to the facts it contains, but it is indispensable that it be legitimate, both in terms of existence, to be among the legally accepted evidence as a means of proof. Or in terms of collection, are obtained by legal means and submitted to the court on the same body as collected, without any change or change during the period of preservation. The main points on which the results were based are:

1. Cybercrime is difficult to detect, as it appears that the number of cases where these crimes have been discovered is small compared to conventional crimes. The reasons for the difficulty of detecting cybercrime can be explained by the fact that this crime does not leave any visible external impact that the offender can commit this crime in other countries and continents, because cybercrime is a transnational crime.
2. After proving the most important challenges facing the security services, and prove that it is more difficult in cybercrime, since the discovery of cybercrime is not easy, and if the discovery of this crime and reporting, the evidence is surrounded by many difficulties, which requires a lot of the neighborhood And technical expertise, which is surrounded by many difficulties, which requires a lot of effort and experience.
3. There is a lack of technical and technical expertise in the police, prosecutors and the judiciary. This is a major obstacle to proving cybercrime. This type of crime requires training and qualification in information technology, evidence collection, research and trial in the computer and Internet environment. Police often fail to assess the importance of cybercrime.
4. Cybercrime may be part of a traditional crime, in the sense that there is a traditional crime involving an electronic aspect, especially since people are connected to new technologies that have begun to spread widely, most notably computers and smartphones.
5. The nature of cyber-crime generally requires unconventional methods of investigation. The discovery and support of digital evidence requires quick action, because electronic evidence is not essential and any evidence or evidence can be eliminated by cybercriminals. Examination, investigation and investigation of traditional crimes, given the glare of cybercrime and immunity.

References

1. Abdul-Jabbouri, Samer Salman (2014) Electronic Fraud Crime Comparative Study, Master Thesis, Faculty of Law, Nahrain University.
2. Adetayo, J. O., S.A. Sanni, and M.O. Ilori (1999). The Impact of Information Technology on Product Marketing: A Case Study of Multinational Company in Nigeria, Technovation, Elsevier Science Ltd.
3. Akpore, S. A (1998). The Backbone of Banks Service Regeneration , Money watch, J 22.
4. Al - Alfi, Mohamed Mohamed (N.D.) Subjective Provisions and Patterns, Working Paper on Legislation Combating Electronic Terrorism Crimes.
5. Al-Afifi, Youssef Khalil Youssef (2013) Electronic Crimes in Palestinian Legislation "Comparative Analytical Study", Department of Public Law, Faculty of Sharia and Law, Islamic University.

6. Al-Balawi, Salem Hamed Ali (2009) Modern techniques in criminal investigation and its role in crime control, Department of Police Sciences, Faculty of Graduate Studies, Naif University for Security Sciences.

7. Ali, Manal El-sayed (2016). The Role of Assistive Technology in the Integration of the Visually Impaired Group with the Availability of Information and Free Trade and the Impediments of its Application in the Arab Countries, Kuwait Annual Conference.

8. Almatarneh, A., (2011) Privacy implications for information and communications technology (ICT): The case of the Jordanian egovernment, Journal of International Commercial Law and Technology, 6 (3).

9. Al-Qahtani, Abdullah Hussein Al-Hajraf (2014) Development of criminal investigation skills in the face of cybercrime. An applied study on the investigators of the Investigation and Prosecution Department in Riyadh, Master Thesis, Police Sciences Department, Graduate School, Naif Arab University for Security Sciences.

10. Arim, Abdul-Jabbar (1970) Theories of Criminology, Dar al-Ma'aref, Baghdad.

11. Ashour, Mohamed Hamdan (2010) Methods of Investigation and Criminal Research, Department of Curricula, Academic Affairs, Palestine Academy for Security Sciences.

12. Attai, Ibrahim Ramadan Ibrahim (2015) Electronic Crime and Ways to Confront it in Islamic Law and International Systems (Applied Analytical Study), Faculty of Sharia and Law, Tanta, Vol. 30, Part 2.

13. Attaran, M. (2003). "Information technology and business-process redesign." Business Process Management Journal 9(4).

14. Badia, Thiab (2014) Cyber Crimes: The Concept and the Causes, The Scientific Forum The crimes that were created in light of regional and international changes and changes during the period from 2-4 / 9/2014, Amman.

15. Beig, Mina, Mohammad Hassan Pourhasomi, Yaser Ghorbanzad (2012). The Role of Information Technology and Customer Relation Management in The Supply Chain, Interdisciplinary Journal of Contemporary Research in Business, Vol. 4, No. 8.

16. Boulmain, Naguib (2008) Crime and the sociological question A study of its sociocultural and legal dimensions, Ph.D., Department of Sociology and Demography, Faculty of Humanities and Social Sciences, Montessori University of Constantine.

17. Bounaara, Yasmina (N.D.) Electronic Crime, Prince Abdul Qader University of Islamic Sciences.

18. Bushati, Brilanda, Damir Šehoviý, and Ilir Binaj (2015). The Importance of Information Technology Use in Business Management, Academic Journal of Interdisciplinary Studies, Vol 4, No 2.

19. Choi, Hyunsang, Hanwoo Lee, Heejo Lee, Hyogon Kim (2007). Botnet Detection by Monitoring Group Activities in DNS Traffic, in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007).

20. Cuel, Roberta ,and Roberta Ferrario (2006) The impact of technology in organizational communication processes: toward constructivism, Italian National

Research Council.

21. Dacey, Raymond, & Kenneth Gallant (1997). Crime control and harassment of the innocent, Journal of Criminal Justice, Elsevier, vol. 25(4)

22. Dilio, Fadel (2010). New Media and Communication Technology, Concept-Uses-Horizons, House of Culture, Hashemite Kingdom of Jordan, Amman.

23. Hassan, Ehsan Mohamed (1993) Criminology, An Analytical Study on the Role of Social Factors in Crime, University of Baghdad

24. Hijazi, Abdul Fattah Bayoumi (2004) Consumer Protection from Commercial Fraud and Counterfeiting in E-Commerce Contracts via the Internet, Third Symposium on Combating Commercial Fraud and Counterfeiting in the GCC Countries, Riyadh, September 2004.

25. Hijazi, Mohamed (2005) Crimes of Accounts and the Internet "Cyber Crime", Egyptian Center for Intellectual Property.

26. Hindi, Amani Ahmed Mashhour, and Basma Salih al-Din Rifai (2017). 5th International Applied Arts Conference, Damietta, Ras El Bar, Applied Arts and Future Prospects, Faculty of Applied Arts, Damietta University.

27. https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime

28. Jain, Neelesh, & Vibhash Shrivastava (2014). Cyber Crime Changing Everything – an Empirical Study, International Journal of Computer Application, Vol.1, Issue 4.

29. Jain, Neelesh, & Vibhash Shrivastava (2014). Cyber Crime Changing Everything – an Empirical Study, International Journal of Computer Application, Vol.1, Issue 4.

30. Jain, Neelesh, Vibhash Shrivastava (2014). Cyber Crime Changing Everything – An Empirical Study, International Journal of Computer Application Issue 4, Vol. 1.

31. Jamal, Brahimi (2018) Criminal Investigation of Cybercrime, PhD Thesis, Department of Law, Faculty of Law and Political Science, Mouloud Mameri University, Tizi Ouzou.

32. Jamal, Brahimi (2018) Criminal Investigation of Electronic Crimes, PhD Thesis, Department of Law, Faculty of Law and Political Science, Mouloud Mameri University, Tizi Ouzou.

33. Kaur, Navneet (2018). Introduction of Cyber Crime and Its Type, International Research Journal of Computer Science, Vol. 5, Issue 08.

34. Kumar, M.Prasanna (2014) Information Technology: Roles, Advantages and Disadvantages, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, Issue 6.

35. Kurt, İbrahim, Hakan GÖK (2015) Impact of Technology on the Perceptions of Culture Shock , Mevlana International Journal of Moral and Values Education (MIJMVE), Vol. 2(2).

36. Lee, Heejin, and Edgar A. Whitley (2002) Time and Information Technology: Temporal Impacts on Individuals, Organizations, and Society, The Information Society, 18.

37. Li, Chu-Fen (2007) The Role of Information Technology in Operating Cost and Operational Efficiency of Banks: An Application of Frontier Efficiency Analysis, Asian Journal of Management and Humanity Sciences, Vol. 2, Nos.

38. Longe, Olumide, Oneurine Ngwa, Friday Wada, Victor Mbarika (2009) Criminal Uses of Information & Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives, Journal of Information Technology Impact, Vol. 9, No. 3.

39. Marquezia, Jean (1983) Crime, translated by Issa Asfour, Oweidat Publications, Beirut.

40. Murtala, Dalhatu Daboh (2005). an Assessment of The Impact of Globalization on Information and Communication Technology (ICT) in NIGERIA, Department of Business Administration, Faculty of Administration, Ahmadu Bello University.

41. Nasser, Mazen Khalaf (N.D.) Principles of Criminal Investigation, Lecture Series for students of the fourth stage, Faculty of Law, University of Mustansiriya.

42. Oluwatolani, Oluwagbemi, Abah Joshua and Achimugu Philip (2011). The Impact of Information Technology in Nigeria's Banking Industry, Journal of Computer Science and Engineering, Volume 7, Issue 2.

43. Research and Studies Complex (2016) Cyber Crime in the Gulf Society and how to face it, the first winner of the competition, Sultan Qaboos Academy for Police Sciences, Nizwa, Sultanate of Oman.

44. Tan, Khong Sin , Siong Choy Chong, Binshan Lin, Uchenna Cyril Eze, (2009). Internet based ICT adoption: evidence from Malaysian SMEs, Industrial Management & Data Systems, Vol. 109 Issue: 2.

45. Tarizi, Nadim Mohammed Hassan (2017) Prosecution authorities pubic in informatics crimes (inspection - inspection), Andalus Journal of Humanities and Social Sciences, No. 13, vol.

46. Thong, J. Y. L. and C. S. Yap (1995). "CEO characteristics, organizational characteristics and information technology adoption in small businesses." Omega 23(4).

47. Tommy, Abdul Razzaq (2006). Information Technology and its Role in National Development - A Field Study in the State of Umm al-Bouaqi, Department of Library and Information Science, University of Constantine.

48. Williams, Luther S. (n.d.). Information Technology: Its Impact on Undergraduate Education in Science, Mathematics, Engineering, and Technology, Report on an NSF Workshop, Directorate for Education and Human Resources, Division of Undergraduate Education.

49. Yeganeh, Mehri Ezadi (2002) The impact of national and organizational culture on information technology (IT), MLS in Library and information Science, Islamic Azad University, Qom branch.