

**“The role of scientific expertise in addressing various issues in their operationalization during emerging crimes “**

**Dr. Benaicha zakaria\***

Dr. moulay taher saida /algeria  
zakaria.benaicha@univ-saida.dz

Received: 17/06/2024 Accepted: 02/08/2024 Published:20/12/2024

**Abstract:**

Nowadays, internet crimes have emerged threatening the security and stability of international community. Criminals, of cybercrimes, have strong opportunity to escape judicial punishment when caught with violations of law, individuals, companies or institutions rights. Cybercrimes are hard to prove through digital evidences of electronic devices. It will be challenging to the authorities if they exclude using modern scientific methods. The latter, however, exposes the link between the crime and criminal therefore, investigator is ought to be well aware of the scientific methods and its role to identify internet criminals as well as the requirements to apply it.

**Keywords:** cybercrime, expert, investigator, electronic proof.

## **1. INTRODUCTION**

Today, the world is witnessing a new massive development in information technology which is considered the Second Industrial Revolution. Therefore, many changes have taken place concerning the way of living, social life and

economic fabric.

The electronic Revolution, however, is unlike Industrial Revolution. It depends on human resources not natural resources. As a result, human brain ability of innovation and development is the core of this revolution and human effort is the mechanism which transfer ideas into accomplishments.

For this matter, the way of investigation as well as the investigator process of thinking has to change too, and evolve accordingly to how cybercriminal thinks. Expert investigation is required for cybercrimes investigation where the investigator reveals the crime and criminals through many procedures and various means necessary to achieve his goal. Investigator, however, cannot do it all by himself, therefore, experts are indeed helpful to ease the task through what is known as the principle of specialization and labor division. We are going to talk about judgeship expertise in cybercrimes through three axes, **axal one** is about the concept of expertness, **axal two**: Internet and virtual world expertness .

## **2. the concept of expertness**

Means, the skills acquired through experience or studying or both on specific domain, therefore, persons with such skills on specific domain are well known as experts. In this paper, we are going to talk about the nature of expertness, the types of expertness, the requirements for tech expert and the fields of expertness in cybercrimes

### **2.1 the nature of expertness**

judgeship expertness is a procedure of investigation confide by

the judge to an expert. It applied when an evaluation and perspective cannot be given by an ordinary person but an expert (**Mahmoud Jamaluddin Zaki ,1990, p11** ) .

Expertness is the mean of which the authority of investigation and the court can provide technical interpretation of evidences using electronic information.

In fact, expertness is a technical evaluation of evidence. Generally, it is a technical report or opinion about crime related matters delivered by expertness. The unique element about expertness is the technical perspective to reveal evidences and its crucial value in proofs, which demands special scientific and technical knowledge of an investigator, or the judge does not have Experience in the investigation procedure.

as stipulated in article 491, "The assignment of experts from the preliminary investigation procedure, if opened by the Public Prosecutor's Office, shall be regarded as an action.

Article 492 further stipulates: "Members of the Public Prosecutor's Office shall refer to the provisions of Act No. 96-52 concerning the organization of experience before the courts.

Judicial expertise requires two pillars. A formality intended to specialize in the level of study and science acquired in the sense that it is acquired by a scientific institution recognized as a university, institute or other. The second element is objective and is intended to be an expert using scientific and practical tools.

If the law takes into consideration the necessity to provide formality and objectivity in expertness, it invites judgeship to

seek classified experts for this matter. This is known as expert roster system, a characteristic of French Institution System. The judge authorizes an expert by resorting to expert roster system which every court has a design about it.

An expert is a person who is well attached to specific science through high technical skill whether by specialized studying or long experience that allows him to be well informed about tiny details ordinary persons are difficult to recognize it. Each expert has its domain when dealing with a case. This is related to what is known as the founding science of academic achievement rule. The field of studying crime has different branches like fingerprints science, pharmacology, analyzing, electronics...etc. all need to be well aware about.

## 2.2 the definition of the expert

The expert can be an employee such as forensic doctor, fingerprint expert and artist engineer. It is highly unlikely to be craftsmen like manufacturer, carpenter or blacksmith. He, however, can be an asset such as professor of university of multiple specialties. An expert is a person who is technically specialized of technical or scientific fields or other areas. Due to his experience and information, he is capable to provide opinion about case related matters where technical expertly is required most (**Omar Ben Younis , 2012, p30**).

The expert is required to combine science and experience. Experience, in some situations, is more valuable than specialty. Science, in our point of view, is insufficient for one to consider an expert in particular field therefore experience is indeed

crucial to support expertness. Logically, give the title of “expert” to newly graduate of university or an academy who has no experience, few years of practice at least, cannot perform well until he acquires much experience while in practice. Under these basis, .( J. Arquilla, & D. Ronfeldt , 1993, p120 )

Law No. 96 of 1952 was issued to organizing experience in front of the judges of the judiciary20/06/1952, In the first article, it stated: **"To carry out the work of expertise before the courts The experts of the current calendar, the experts of the Ministry of Justice, the Department of Forensic Medicine and other interests entrusted with the work of expertise and all those who see the courts as necessary to use their technical opinion from those not mentioned."**

Articles 292,293 of the same Act stipulate the court's right to assign experts at the request of the adversaries or on its own initiative. As noted, the articles on experts are contained in chapter III, chapter III, of the Code of Criminal Procedure. The provisions of this chapter contain detailed provisions on the use of experts before the criminal courts .

The cassation judgement therefore established that the provisions of the present chapter must be followed before the courts and supplement the aforementioned articles.

## 2.3 Expert types

Experts can be divided into two types: the first category: police officers experts who work in the field of forensic lab and criminal evidence. They are required to have specialized

training such as studying chemistry, nature, engineering, and photography to add scientific analysis in the field of expertly.

This category specialized for the inspection fire arms, the exposure of forgery and falsification, font emulation and the inspection of combustion cases. The second category, are graduates experts of practical universities such as medicine, engineering and science who are taught some legal and police matters in accordance to what they need in inspection field (Hassan Allam , 2013, p192 ).

#### **2.4 The requirements for the informal expert**

Qualities for the experts can be summarized as follows:

- 1- Commitment to the rule, laws and regulations, particularly, the Code of Criminal Procedure and the Law of Proof of Civil, Trade Courts and the Anti-Cybercrime Law.
- 2- the well knowing of electronic investigation and the means of finding evidence to reveal the criminal.
- 3- Take advantage of all the trails on crime scene whatever size it was.
- 4- Evidence evaluation in terms of importance and its effect on the incident.( Y. Barthe & C. Lemieux , 1999, p200 ) .
- 5- Must be patient and persistent with high focus on analyzing tiny trails or details.

- 6- He must identify the circumstances of the incident from the moment it took place to the moment was discovered and the sides involved as well as the purpose behind it.
- 7- The expert must not make conclusions base on interpretations without deep scan of evidences. He must be honest and faithful in his job, seek always the truth and fulfill justice.
- 8- He must step aside when interest conflict occurs.
- 9- He must avoid being in places and with persons of suspicion
- 10- while working, he must not get involved with persons related to the incident that would soften his judgment or lead to personal interests.
- 11- he must know technology and have a good background about new science under expirementation.( **Y. Barthe, M. Callon& P. Lascoumes, 2002, p80** ).

## **2.5 the fields of expertness in cybercrimes**

The areas that need expertness do vary. It might include state employees or others such as forensic doctors who receive specialized formation on types of felonious wounds where their expertly clarifies the reasons behind the wound or death, the way it happens, the tool that was used, the timing of the incident and the consequences. In addition, the fingerprints experts expose the prints on the crime scene and compare it with other fingerprints of suspects and other criminals. Moreover, photography experts take the responsibility to

photograph the crime scene and its components. They, as well, elicit some trails and deposits, therefore, they record the whole crime scene through photography. Investigators and court are, therefore, teachable about crime scene in full (U. Beck, 2009, p200 ) .

Criminal experts such as biological testing experts and chemical testing experts whom job is to analyze organic matters or other in order to identify its known and unknown components. Firearms experts, identifies the type of weapon, firearm chuck used in shooting. They result to whether it is compatible to the firearm used or not. They, also, study the shooting angle or the position the criminal and suspect held during the crime (D. Bigo, 2005, p205 ) .

Combustion experts reveal the materials used in incineration. They also seek whether the incineration was deliberate or a result of electrical contact as well as identifying the starting point of inflammation, the reasons behind it and the amount of time of materials used in inflammation or the amount of time of the whole fire taking place.

Fabrication and forgery experts identify the forgery by studying the data where forgery happen or determine the original copy from the fake one. This, however, requires various technical and modern ways to fulfill.

Other categories of experts, who may not be part of governmental body, are considered as qualified experts. When investigator cannot provide a proper judgment on specific matter, he resorts to such experts to give their evaluation based

on their knowledge. These categories of experts can be animal breeders of sheep, camels, pigeon...etc. Their expertly is needed to determine the value of the wounded animal or its death caused by the illegal action of the suspect ( **S. Brint, 1994, p70**) .

## **2.6 experts in cybercrimes**

Experts are invited only when necessary or when special circumstances occur. Inviting experts must be under traditional criminal procedures. In my view, the use of experts in accordance with the traditional approach to criminal proceedings is in fact linked to a traditional logic that the procedural legislator must change in order to allow it to be bypassed in the context of cybercrime.

In addition, no law forbids the trial court to authorize experts out of the expert list. However, this approach need to be developed to ease the use of experts without providing logical reasons to do so.

The development must include international authorization of experts from another region when dealing with cybercrimes. This is possible in virtual world for it is a whole connected digital environment. For example, seek help from governmental bodies, institutions and private institutions which are active in information technology. Using internet to reveal ambiguity cost less. All what is needed is the availability of communication environment using information technology and the internet. If digital environment is provided, the legislation about this approach can be issued to serve its purpose legally.

Investigator must be knowledgeable about cybercrime as a result, he should seek help from another expert about some matters but not for the whole investigation. This would look like the investigator is using a consultant to do his job when, in some legislations, only the suspect has the right to do so. The law has allowed investigators to authorize experts when urgent matter occurs that requires incident clearance based on scientific explanation (knowledge) **(P. Collier, 2006, p150).**

The law gave authority of investigation to the accusation room. It is the second grade of investigation degrees and has the jurisdiction of investigative judge plus legal jurisdiction. The law, therefore, authorizes the accusation room to review the investigation conducted by investigative judge or public prosecution. Then, it can seek help from experts. The trial court is the main authority that law allows to hold an inquiry in the course of investigation **(Omar Mohamed Abubakar Younis, 2004, p70 ) .**

No law denies the suspect his right, as well as the defense, to run an investigation about the accusation on him which provides a bigger opportunity to his defense to establish justice. The suspect has the right to attend the course of investigation and trial and be invited by the investigative side.

Consultancy expertise is an activity done by the suspect in order to defend his right, however, it depends on the nature of the lawsuit. Therefore, argue that consultancy expert is available at the court expert's disposal is flawed argument. This argument, restrain the right to create. The law has never restrained it but gave unlimited power to assign consultancy

expert or more. As we mentioned above, sometimes investigator has no clue or little knowledge about certain crimes such as cybercrimes. As a result, a certain question was raised, does the law permit the investigator to assign consultancy expert for the matter under investigation? (**B. Dupont & V. Gautrais , 2010, p300 ) .**

consultancy expert has two objectives. First, the clarification of the incident. Second, reveal the ambiguity about certain incidents. In cybercrimes, consultancy expert clarifies how internet works then suggest his point of view about mysterious sides of cybercrime. As a result, consultancy expert is ought to be well skilled when the judicial expertness is not enough (**ENISA, Annual Incident Reports 2012, p123 ) .**

The question, therefore, is raised; to what extent investigator can engage consultancy expert during investigation?.

In fact, the assignment of consultancy expert is one the strength points which characterizes the states that are still on the digital or technical growth phase. Such matter, if come into effect, will raise lot of procedural issues (**Omar Mohamed Abubakar Younis, 2004, p891 )** for, the defense can seek explanation of the basis of conclusions achieved by the investigator, therefore, the defense can argue that the investigator or prosecution expresses a logic beyond the realization of a judicial charge. Legislator need to intervene and make consultancy expert an asset to the evidentiary sides to investigation and prosecution not for the suspect only. And, authorize digital consultancy expert as full expertness unrestricted

### **3. internet expertness field and virtual world**

The tech expert examines various device through specific ways. We will go into some details on the following **(D. Garland, 2008, p305 ) :**

#### **3.1 devices examined by tech expert**

Many devices are subjected to forensic medicine examination to identify the main proof used to commit cybercrimes. Among which, answering machine, mobile phones, pager, digital camera, printing machine, fax, GPS, scanner, laptops and other devices that may be used by the suspect to commit the crime. The computer, however, is main important unit in terms of storing information. To this end, a certain question is raised, to what extent can justice resort to expertness when the law oppose one of the cybercrime topics while facing a new emerging topic of virtual and digital world at once?. this means, the expertness standards of today, can raise debate about it, will be different in the future **(C. Gilbert, 2011, p50 ) .**

Tech expertness in the field of internet and virtual world does not necessary require experience coursework. Computer science and internet has no curriculum, field of research or an amount of time one spends in universities or specialized is institute to be eventually an expert. However, it requires unique skill and talent in using computer, internet and dealing with tech information. For instance, Bill gates, the best programmer so far, his academic achievement never surpass secondary school.

The thing for hackers, their academic achievement never surpasses secondary school or the first years of university, at best situations. Therefore, expertness in tech information is different than any expertness branches used by justice (F. Guarnieri & E. Przyswa, 2011, p50) .

### 3.2 types of techs expertness

- a- **Personal expertness:** it is one the most powerful expertise (F. Guarnieri & E. Przyswa, 2011, p90) in terms of creating competition among private organizations. It includes individual expertness, outlaws as well, which is the main manifestation in techs information and internet.

An economic approach, however, calls to keep such talented individuals to go unpunished by law but working to serve economic goals instead. Moreover, some states are trying to identify hackers who become national symbols due to their activity in internet. In addition, private organizations seek to be leading the way of expertness as well. It has different objective. On the one hand, some non-governmental organizations seek to encounter any violations of digital rights by criminals. On the other hand, some organizations seek to decode virtual world ways to serve its commercial basis (Hussein bin Said bin Saif al-Ghafri 2015,p442) .

- b- **Educational institutions body:** it is crucial asset for it is a non-commercial institute. It is a supplementary source for state institutions where its purpose is science development to eradicate humanity issues as possible. Scientific thinking is unavoidable in order to note human phenomena as well as

cybercrime development. Therefore, educational institutions are to be supported, financially and morally, to better its role, mainly, financial and monetary crimes...etc. Information technologists are the best to decode cybercrime secret. Many institutions have formed large expertness base to deal with cybercrime challenge, among which, supercomputing science in Stanford University, Massachusetts Institute of Technology which introduced high quality of experts to humanity.

**c- Criminal investigation body:**

Some states have initiated institutions for cybercrime expertness. The USA is on top of this matter. It created an international body known as the Interpol. The U.S. government created another FBI branch known as the Legitimate Regional Computer Laboratory (**The regional computer forensics. Laboratory TE.USA. cyber criminalite, 2000, p234** ) , San Diego. It was introduced in November 2000 to serve as a multiple source of expertness its purpose is to fight the dangerous escalation of cybercrime. It analyzes and classify digital evidences through Computer Forensics Examiners who will be of great importance to intensify the fight against cybercrime. The new forensic laboratory is meeting and corporation point of many criminal investigation bodies to benefit more such as Drug Enforcement Administration (DEA), Defense Criminal Investigative Services, US Customs Services, Naval Criminal Investigative Services, the Office of Attorney General for Federal District, the District Governor's office and California Administrative Agency (**Jerry seper, 2000** ) .

### 3.3 The Means of Techs Expert

The techs expert has to do whatever necessary to seek the truth. Scientific tools are required to do his job. The court, in return, cannot deny these without a logical reason, otherwise, there will be a cassation appeal against its verdict.

The Techs Expert has two ways to pursuit his job (**Omar Mohamed Abubakar Younis, 2004, p42**) :

First, collect the scene where the crime is shaped such as intimidation, fraud, defamatory, Infringement of copyrights and the incitement to prostitute, human trafficking or child prostitution...etc. Then, initiate digital analytical process to reveal its programing that will lead to the way it was made or prepared, define its pattern, how its recognition works and finally, decode the Internet IP protocol which identify the computer responsible. Second, collect the sites that are not crime scene but a cause to the crime. These sites do vary such as sites that help to recognize drugs doses and psychotropic substances. These sites promise, in tricky way, its users that following them will cause no addiction. Sites that teach the illicit drug cultivation and how to hide it. Sites that teach bomb-making, how to deal with time bombs and how to compose and recompose bombs (**Patrick S, Chen, 2000, p164**)

Sites that determines the route of entry on prostitution sites from different places It is also necessary to determine the course of entry on prostitution sites from different locations without the need to determine the route of entry from a fixed location. Such an order may occur as if the perpetrator was a

participant of a provider in a city different from the one in which he resides and accessed the Internet from his place of residence. The latter is one of the defences to which the court in question is obliged to respond (F. Guarnieri & E. Przyswa 2012, p312) .

### **Expertness in cybercrimes helps as follows:**

- 1- Reveal the digital evidence
- 2- Test its originality through scientific and technological means so law can be applied on
- 3- Identify the unique characteristics of digital evidence.
- 4- Repair the evidence and re-collect it from hard drive
- 5- Make original copy of digital evidence in order not to lose any information while recovering the evidence
- 6- Collect digital cyber trails that may have changed during information network.
- 7- Use algorithm to confirm that evidence has not been messed with or modified .
- 8- Confirm that the evidence is reliable and a submitted part within criminal proceedings
- 9- Classify the special characteristics for each cyber evidence such as digital files, applications, contacts, photos, audio...etc (Hussein bin Said bin Saif al-Ghafri, 2015, p398) .

### **3.4 the means of tech expert in decoding digital evidence:**

The expert deploys many means to catch the cybercriminal and

the way crime took place. We address as follow :

First: Material Means: it is the technical tools that are usually used in information system structure. It can be used to investigate and confirm that the crime has taken place such as:

1- IP, e-mail and chat applications:

The IP is the responsible of messaging data packages via the internet and directed to its pathway's targets. It is similar to the mail address which allow to transfer the message. It exists in every device connected to internet. It is composed of three parts. Each part is composed of four column. The first part, from the left, indicates the geographical area. The second part indicates the server. The third part indicates the number of connected computers. The fourth part indicates the computer where the connection was made (Mohammed Amin al bushri , 2000, p186 ).

If any problem occurs or acts of sabotage, investigators must search the device number and locate it to identify the suspect responsible. Internet server as well as phone service network can track the accomplice as long as special equipment is available. The ways to know IP address do vary. For instance,

There is more than one way that you can find out about this computer address in case of direct connection than, for example, what is used in case of working on Windows operating system where WINPCFG is written in the operating order to show a dialog between the IP address while noting that the Internet address may change with each Internet connection In the event that an interactive programme is used as a crime

tool, it requires the identification of the caller. The email also identifies the addressee's personal address, even if the addressee's information is not recorded in the addressee's box, provided that the information placed at the email settings stage is correct. (Jameel Abdel Baki Al-Saeir, 2002, p82 ) .

## 2- PROXY

The Proxy works as mediator between the network and its users where large companies guarantee its capability to manage the network and provide Cache Memory. The Proxy idea stand on the user request for Proxy server to look for a page inside local memory cache. The Proxy checks if the page was downloaded before, then send it to the user without send the request to the Global Company. In contrary, the user request is sent to the Global Company. The latter works as customer server and uses an IP address.

The proxy memory cache can save operations done within, which makes powerful proof through the examination of suspect saved operations in the proxy.

- 3- Backtrack programs identify the penetration attempts and notify the user with notice details of the incident, date of the incident, address through which penetration took place, the internet company name and entrance and exit numbers on the network...etc .
- 4- Intrusion Detector System (DS) : it supervises ongoing operations on computer or the network. It searches for any problem signal that may menace the computer or network 37. It analysis the data during the transfer process on network and

event recorded folders when taking place on computer or network. In addition, it compares analysis results with a group of common incidents of assaults which happened on computer systems and it is known among specialists, the signature. If the system discovers one of these signatures, it warns the system manager through different ways and record the data related to the assault in the computer special folders (Bace, Rebecca 2000, p116).

Second: executive means:

The procedures used are intended to implement established, specific, variable and undefined investigative methods that establish the occurrence of the crime and determine the perpetrator's identity.:

- 1- Cyber criminals are afraid of tracking when committing a crime for many documents that give pieces of advice of what to do. The most famous one is “cover your track” document which teaches cybercriminals how to not get caught. Tracking can be through email or the device used for the cybercrime.
- 2- Investigator should be knowledgeable of cyber system and its components of network, applications and customer service.

He should as well knowledgeable about data base, its administration, its insurance plan, system materials, users, beneficiaries, folders, procedures, material classification, synchronizing devices, specific time used for passwords, the extent of distribution of competence for beneficiaries, security measures of personnel, back up method and use protection program to supervise such as beneficiaries, resources, data

processor, incidents recorder and failure attempt to broke in into system.

- 3- The AI has proven successful in collecting criminal evidences and reach conclusions about facts. It is important to narrow the cercle of facts, possibilities and assumptions then reach conclusions through calculations that are calculated by specific programs ( Jameel Abdel Baki Al-Saeir , 2002, p82) .

### **3.5 The Role of Technical Expert in Keeping cyber evidences**

Evidences of internet crimes vary. Some need to be kept inside the computer, others need to be kept in the virtual world and special evidences belong to the digital world. However, evidences can be transferred into real world where it can be considered as full evidences help in conviction or prove innocence (S. Leman-Langlois, 2006, p99 ).

Preserving computer evidences is a complicated operation which needs a precise observation to the authenticity of data on computer. The techs expert need to confirm that the computer preserved evidences is cleaned of virus for it can damage evidences, therefore, its reliability. This is well known in the English Legislation. Computer evidence preservation is done through simple way by the common procedure of saving or computer locking of evidence. The digital evidence is usually a folder contains digital data indicates to specific information that cannot be changed unless it is modified ( OCDE, 2010, p217) .

In order to preserve evidences, the expert techs need to observe

the internet site or information which indicates the crime, manifested in various forms. When defamatory and insulting in chat room happen, the server memory is way to indicate the topic of defamatory and insulting topic, the date and whether the type of crime. In this case, the techs expert can use the computer memory without using the server...etc. He is going to use helping programming to reach the value of preserving evidences in digital world. As in the case of the seizure and encryption of such sites after the enumeration of their polemics, accuracy and trajectory, this is a presumption that they were the perpetrators of the crime. Preserving evidences in digital world invite techs expert to present it to the court or investigative bodies. This will keep techs expert carrying on his job until the trial take place.

As in the case of the evidence submitted to the trial court before a higher judicial authority (such as appeal or cassation in the case of its jurisdiction - appeal twice).

#### 4. CONCLUSION

The technological revolution has triggered crimes of different nature yet the procedures to detect these crimes are still traditional by using methods meant for traditional crimes not emerging crimes.

This matter can lead to various problems in terms of detecting cybercrimes of moral entity which do vary. It is possible to take place in several places in just one country.

It can occupy wider range to include many countries such as money laundering via internet, therefore, taking procedures against it is inaccessible or might be illegal to do so.

As a result, Germany doctrine, in some situations, questions the possibility to log into information technology system to adjust stored data without the consent of the concerned country.

It is a violation of the country's sovereignty and bilateral agreement of justice corporation.

It is well observed that inspecting for cybercrimes evidences violates the right to privacy.

Inspection is conducted, often, on computer systems, data base and network information which may overpass the information system, under suspicion, to other systems in relation due to the common networking between computers and the spread of internal networks on the institutions, local networking,

local network, regional and international level. This, however, will lead to violate digital privacy rights when inspection comes into effect.

Scientific expertise is paramount in addressing and mitigating emerging crimes, which are increasingly complex due to technological advancements and global interconnectedness. To effectively operationalize solutions to these issues, the following recommendations are essential:

- **Strengthen Multidisciplinary Collaboration:**
  - Encourage partnerships between scientists, law enforcement, policymakers, and technologists to

foster a holistic approach to crime prevention and resolution.

- Develop integrated platforms for real-time information sharing and joint task forces that include scientific experts across relevant fields.
- **Enhance Education and Training:**
  - Implement comprehensive training programs for law enforcement and legal professionals to understand the nuances of scientific methods and technological advancements.
  - Promote continuous professional development to keep up with the rapid pace of change in scientific research and its applications.
- **Invest in Research and Development:**
  - Allocate substantial funding for research into emerging crime trends, innovative detection technologies, and forensic methodologies.
  - Support public-private partnerships to drive innovation in crime-fighting tools and techniques.
- **Develop Robust Legal Frameworks:**
  - Update and create laws that reflect the realities of emerging crimes, ensuring they are flexible enough to adapt to new scientific findings and technologies.

- Ensure that legal standards for evidence collection, preservation, and presentation in court keep pace with scientific advancements.
- **Promote Public Awareness and Engagement:**
  - Launch public education campaigns to raise awareness about emerging crimes and the role of science in combating them.
  - Encourage community involvement in scientific initiatives aimed at crime prevention and safety enhancement.
- **Enhance Data Analytics and Cybersecurity:**
  - Invest in advanced data analytics to predict and prevent crime patterns, leveraging big data and machine learning.
  - Strengthen cybersecurity measures to protect sensitive information and infrastructure from cybercriminals.
- **Foster Ethical Standards and Accountability:**
  - Establish and enforce ethical guidelines for the application of scientific expertise in law enforcement to prevent misuse and ensure public trust.
  - Implement mechanisms for accountability and oversight to maintain high standards of integrity and transparency in scientific practices related to crime prevention.

- **Global Cooperation and Standardization:**
  - Promote international collaboration to address transnational crimes, ensuring consistent standards and practices across borders.
  - Share best practices, technological advancements, and research findings through international forums and collaborative networks.
- **Utilize Forensic Science Advancements:**
  - Invest in the latest forensic technologies, such as DNA analysis, digital forensics, and biometric systems, to enhance investigative capabilities.
  - Ensure forensic laboratories are equipped with state-of-the-art tools and staffed by highly trained professionals.
- **Support Evidence-Based Policy Making:**
  - Encourage policymakers to rely on scientific evidence when drafting and implementing crime-related policies.
  - Conduct regular evaluations of crime prevention programs to assess their effectiveness and make data-driven adjustments.
  -

## 5. Bibliography List :

- Bace, Rebecca (2000) Interusion Detection, Indianapolis, Indiana

- Jameel Abdel Baki Al-Saeir, (2002) , procedural aspects of cybercrime, Arab Renaissance House,
- Mohammed Amin Al-bushri , ( 2000) , Investigating Computer and Internet Crime Research published in the Arab Journal of Security Studies and Training, No. 30 Naif Arab University of Security Sciences, Riyadh.
- OCDE, (2010) , Conference on empowering e-consumers: strengthening consumer protection in the Internet economy, Summary of key points and conclusions.
- S. Leman-Langlois. (2006) , « Questions au sujet de la cybercriminalité, le crime comme moyen de contrôle du cyberspace commercial », Criminologie, vol. XXXIX, n° 1, printemps.
- B. Dupont & V. Gautrais,( 2010) , « Crime 2.0. le web dans tous ses états », Nouvelle revue internationale de criminologie, vol. VII,.
- C. Gilbert, (2011) , Conférence Mines ParisTech De la gestion des risques à l'organisation de la résilience. Implications d'un changement de perspectives.
- Counsellor Hassan Alam, ( 2013 ) , means of probation in cybercrime. Noffel Foundation, Beirut, Lebanon.
- D. Bigo, (2005 ) , << La mondialisation de l'(in)sécurité ? Réflexions sur le champ des professionnels de la gestion des inquiétudes et analytique de la transnationalisation des processus d' (in)sécurisation », Cultures & Conflits, n° 58.
- D. Garland, (2008), << On the concept of moral panic >>, Crime, Media, Culture, vol. IV, n° 1.

- ENISA, Annual Incident Reports, octobre 2012
- F. Guarnieri& E. Przyswa, (2011), « Cybercriminalité contrefaçon: les interactions entre réel et virtuel' », Cahiers de la sécurité n° 15.
- F. Guarnieri& E. Przyswa, (2012), « Cybercriminalité et contrefaçon pour une nouvelle analyse des risques et des frontières », Murs et frontières, Hermès, n° 63.
- Hussein bin Said bin Saif al-Ghafri, ( 2015) , Criminal Policy in the Face of Al Obeikan Internet Publishing Crimes, riyad kingdom of Saudi.
- **J. ARQUILLA, & D. RONFELDT**,(1993) « Cyber war is coming!» Comparative Strategy, vol XII, n° 2, printemps.
- Jerry seper, ( 2000), FBI steps up efforts to fights crimes related to computers, the Washington times, available on line nov. at: <http://www.infowar.com>

**MAHMOUD JAMALUDDIN ZAKI**, (1990) , experience in civil and commercial materials , publishing house Cairo University.

Mecmil lab Techniccat Publishing.

- **OMAR BEN YOUNIS**, ( 2012) , Criminal Proof Online, i 1 Dar Al-Thakr University Alexandria,.
- Omar Mohamed Abubakar Ben Younis, (2004) , Crimes arising from the use of the Internet Substantive Provisions and Procedural Aspects University of Zagaziq Faculty of Law,.
- P. Collier. (2006) , << Spécial Internet: Fin de l'immunité pour les opérateurs techniques? >>, Contrefaçon Riposte, n° 18/19.

- Patrick S, Chen - An Automatic System for Collection Crime information on the internet 15/06/2024 Journal of information Law and Technology Available online in juin 2024. at: <http://elj.warwick.ac.uk/jilt/-3/chenhtml>
- S. Brint, (1994 ) In an Age of Experts. The Changing Role of Professionals in Politics and Public Life, Princeton, Princeton University publish .
- The regional computer forensics. Laboratory TE.USA. cyber criminality.
- U. Beck, (2009) , contre-pouvoir à l'heure de la mondialisation, Flammarion Pouvoir et Champs Essais, .
- Y. Barthe & C. Lemieux,(1999) « Les risques collectifs sous le regard des sciences du politique. Nouveaux chantiers, vieilles questions », Politix, n° 44.
- Y. Barthe, M. Callon& P. Lascoumes, (2002) « Réponse à Franck Aggeri », Gérer et comprendre, n° 68.