



**Kingdom of Morocco
Ministry of Justice**



**United Nations
Development Programme**

**PROGRAMME ON STRENGTHENING THE RULE OF LAW
IN ARAB STATES – PROJECT ON MODERNIZATION OF
PUBLIC PROSECUTION OFFICES**

**Regional Conference
on CYBERCRIME**

**19-20 June 2007
Casablanca, Kingdom of Morocco**

EXPLANATORY NOTE

1. Introduction

The United Nations Development Programme - Programme on Governance in the Arab Region (UNDP-POGAR) launched an initiative to modernize and develop the activities of the public prosecution offices in the Arab countries and to activate the role of the public prosecutors in strengthening the rule of law and good governance.

The Project seeks to achieve four main objectives, namely:

1. Building and developing the capacity of public prosecution offices.
2. Creating and promoting relations of cooperation between the public prosecution offices and civil society organizations to secure a better application and protection of the rights of citizens.
3. Creating a regional and international network for cooperation among the public prosecution offices in the field of crime prevention.
4. Reforming laws that govern and regulate the work of the public prosecution offices, the criminal court, and the adopted practices.

In this context, several activities were implemented. They included holding workshops and training courses to educate the public prosecutors about modern crimes, in general, and the advanced investigative methods and techniques.

As part of the Project, a regional conference was held in Cairo on 28-29 March 2007 on transnational organized crime as this type of crime is on the rise, particularly, trafficking in persons, drug abuse, and terrorism. In addition, it has negative impacts on both the individual and the society, let alone the key role *niaba* (the public

prosecution institution) plays in the prevention of this type of crime. The conference yielded valuable results and recommendations which the participating countries have committed themselves to respect and put into practice¹.

Within the context of building the capacities of the public prosecutors, and as part of the Project, a second regional conference on “Cybercrime” will be organized in Casablanca, Morocco, on 19-20 June 2007. The purpose of the conference is to disseminate knowledge about cybercrimes, exchange ideas among the participating public prosecutors, and create a framework for cooperation for combating these crimes and curtailing their growth.

The conference will focus on the following themes:

1. General introduction to cybercrimes: definition and forms.
2. Legislation related to cybercrime and the importance of introducing a national legal framework comprising all these forms of crimes.
3. Building the capacities of the human resources in the field of investigation, prosecution, and trial of cybercrimes.
4. Procedural safeguards and international cooperation in combating cybercrimes.

2. Background

The world is currently witnessing, under a new era, the symptoms of scientific renaissance which are mainly represented in the emergence of the computer and the associated great advancement in the field of internet and communication. Indeed, the big development in communication has turned the world into a small village. One can now watch what is happening on the other hemisphere in sound and picture at the moment an event occurs. The exchange of information and knowledge has become easy and fast with the use of modern communications methods.

Computers are no longer used only for conducting the sophisticated computation processes but have extended to include issues of interest to the people in all their commercial, banking, and other transactions. This big and accelerating development of the role of the computer has added to humans huge capabilities to store and process information in speed beyond imagination. Parallel to this development, the people’s awareness of the importance of information as a source of power, and sometimes of wealth, has also increased.

Indeed, we live today the age of information revolution which is taking amazing big strides. The trade of information represents 8% of the value of the international trade. Hardly is there an economic, social, industrial, or administrative field which the computer and information technology do not play a key role in its performance and development.

¹ For the full text of the recommendations, see the Project’s site: <http://www.arab-niaba.org/publications/crime/cairo/recommendation-a.pdf>

As a result of this development in the information field, new types of crimes have emerged and grew which would not have come to existence without the emergence of computer and the stunning advancement caused by the use of the internet. Various types of these crimes emerged and took different shapes. A problem, thus, appeared in terms of identifying and classifying these crimes. Do these crimes belong to crimes committed against property? Or against persons? Or against the public interest? Are they conventional crimes? Or economic crimes? Or do they constitute a new type of crime? These crimes took different labels; for example, piracy. Their perpetrators are perceived as intruders who are divided into three sub-divisions: the first group violates the security of networks; the second violates the security of software applications; and the third devises software which destroys computer's hard disks, etc.

The world has looked with gravity to the cybercrimes and has been attaching great attention to their prevention since the end of the 20th century. Perhaps the most outstanding effort for preventing these types of crimes was the conclusion of the Convention on Cybercrime issued by the Council of Europe in Budapest, 23 November 2001². The Convention is the only multi-party Convention on cybercrime prevention and, therefore, has motivated other countries outside the Council of Europe and the European continent to join it. On 22 September 2006, the United States joined the Convention and ratified it as of 1 January 2007.

The international attention given to the Convention on Cybercrime has turned it into an international document binding on the states party to the Convention. Many states, which are not members of the Council of Europe, seek to join the Convention.

The Council of Europe's Convention on Cybercrime expressed the realization by the Council's states of the new dangers posed by the rapid growth and spread of the computer networks. According to the Convention's Preamble:

The member States of the Council of Europe and the other States signatory hereto,

Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;

Conscious of the profound changes brought about by the digitalization, convergence and continuing globalization of computer networks;

Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences.....

As regards the Arab region, so far there is no convention or draft convention dealing with Arab regional cooperation on cybercrime prevention. It is, therefore, important to increase awareness and knowledge about this aspect in the Arab region. There is also an emerging need to train the law enforcement agencies and prosecution offices on these types of crimes, particularly, in the light of the rapid developments in the world.

² To see the full text of the Cybercrime Convention, see the Council of Europe's site: <http://www.conventions.coe.int/treaty/EN/treaties/html/185.htm>

DRAFT

Particular mention is made here to the globalization phenomenon and the rapid movement of information and data across the national borders from one country to another.

3. Objectives

The main objective of the conference is to educate the members of the public prosecution offices about cybercrimes. The conference seeks, in particular, to achieve the following:

1. Study the concept and types of Cybercrime in terms of their definition, forms, way of implementation, threats and challenges they pose.
2. Support the capabilities of the national criminal systems to combat these crimes by informing the judges and public prosecutors about this new type of serious crimes, mechanisms of their prevention, investigation techniques, particularly, in terms of information gathering and evidence evaluation.
3. Provide the appropriate training to the members of the law enforcement agencies in investigating and prosecuting these crimes. This includes training on adopting special techniques of investigation in combating this type of crime which is committed through the computer and the internet away from the eyes of the law enforcement authorities.
4. Shed light on the international standards in this connection, the governing principles, the types of committed crimes, and the prevention mechanisms.
5. Highlight the legislative reality in the Arab countries and focus on the need to adopt new legislation at the national and regional levels in the field of combating these types of crimes in line with the criminalization and prevention efforts made at the international level.
6. Establish rules for regional and international cooperation in the protection of technology and prevention of cybercrimes.

4. Conference material

The conference is centered on cybercrime in terms of its definition, types, threats at all levels, reasons for legislation, and methods of prevention.

Therefore, the conference will address the conventional crimes committed through the use of computer and those affecting the freedom, security, safety, and availability of the computer data and systems.

Further, the crimes of copyright infringements and related crimes, pornography-related and child pornography crimes will be discussed. Each crime will be dealt with separately whereas experts will define each crime and shed light on its elements, development, way of implementation, methods of prevention, investigation, and gathering of evidence to bring it before court and punish its perpetrator.

Finally, the conference will discuss the national legislative reality in the Arab countries in respect of cybercrimes compared to the international legislation in this connection. Light will also be shed on the measures and mechanisms of prevention of these crimes and of the dangerous threats they pose at the international level.

The following are the details of the above themes that will be discussed in the conference:

A. General introduction to Cybercrime: definition and forms

a. An overview of information technology and related crimes

The term Information Technology (IT), or *informatique*, was used for the first time by Professor A. I. Mikhailov, Director of the Federal Institute of Scientific Information and Technology (VINTTI) in the former Soviet Union, to describe the science of scientific information³. The term was then used at a broader geographical level in different concepts to the extent that more than 30 different definitions were given to the term in the specialized writings on information science.

According to the French Academy, IT is defined as “the rational dealing, particularly by automatic machines with information as a mainstay for human knowledge and a pillar for communications in the fields of technological, economical, and social fields⁴.”

UNESCO has a broader and more advanced definition of information technology or the so-called *informatique*. According to UNESCO, the term incorporates the scientific, technological, and engineering branches and the methods of management used in handling information processing and applications. It also encompasses the computers and their interaction with man and machines and the associated social, economic, and cultural matters⁵.

Many definitions were given to the IT-related crime, which vary from narrow to broad in scope. However, generally speaking, IT-related crime can be divided into the following four categories⁶:

1. Definitions centered on the method of committing the crime.
2. Definitions centered on the object of the crime.
3. Definitions related to knowledge about information technology.
4. Mixed and various definitions.

b. Types of cybercrimes

The object of cybercrime differs depending on whether the object of the crime is a component of the information system or the crime’s perpetrator (who used that system

³ [Tr. Russ. Informatika (A. I. Mikhailov et al. 1966, in *Nauchno-tekhnicheskaya informatsiya XII*. 35), f. INFORMATION: see- ICS.]

⁴ In France, the official use of the word *informatique* was adopted by the Council of Ministers and, then, by the French Academy in the year 1967. See: <http://www.academie-francaise.fr>; <http://fr.wikipedia.org/wiki/Informatique>

⁵ www.unesco.org

⁶ Jurists, particularly French jurists, divide information crimes into two categories; 1) crimes committed by information technology; and 2) crimes where information is the object of the crime. See:

- Andre Lucas, Jean Deveze, et Jean Frayssinet, *Droit de l’internet*, PUF, Themis Droit Prive, 2001, pages 663 et s.
- Vivant, Le Stanc et al : *Lamy Droit de l’informatique et des reseaux*
- N. Huet et Maisl : *Droit de l’informatique et des telecommunications*, Litec. 1989, p. 833 et s.

and was the method to implement the crime). In the first case, the pure conventional crimes are combined with the cybercrime in its technical meaning. The former exists if the hardware of the system, such as the sets, equipment, and cables, are the object of assault or of crime and little consideration was attached to the technology in committing the crime. An example of this case is the theft or destruction of a computer or a monitor.

The second case exists where the intangible components of the system, such as the data and software *per se* are the object of assault. An example of this case is when an assault is committed against the data stored in the computer's memory or transmitted through the communication networks by theft, forgery, or assault on the software themselves by claiming their ownership, or stealing, reproducing, destroying, deleting, or obstructing them. It is the forms of the second case (i.e. assault against the data and software), not the first one, that, due to its relative modernity, has not been addressed so far in most of the existing penal codes.

In the second case; i.e. the crimes committed through an IT system so that it is the method and tool of implementing the crime, the committed crime is conventional but the tool and method of committing it is the computer or the IT system. In theory, as testified by some cases in reality, a computer can be used for committing a variety of crimes, such as remote coordination of the activities of terrorist and organized crime groups, robbery of banks, conclusion of mock transactions in the names of other persons, fraud by use of IMT cards, money laundering, threats of murder, stimulating sexual instincts, and publishing materials offending the public morality.

Here, the perpetrator of these crimes manipulates the computer and its system. However, the material object of the crime, of course, differs depending on the thing which is targeted by the perpetrator's conduct and which constitutes the object of the right or the protected interest.

c. Challenges posed by cybercrimes

The widespread use of computers poses associated threats to different social and individual interests which the community seeks to protect. Use of the computer has increased to the extent that it has become crucial to the life activities in the community, particularly the economic, commercial, cultural, and scientific activities and even the individuals' activities in their personal lives. This penetration of the individual's and community's life obviously testifies to the emergence of new values linked to that set, particularly, the need to care for and protect that achievement from assault.

Assault against computer systems can threaten life of paralysis. It is not an exaggeration to say that tampering with the computer systems can be a threat to the international security and peace as many weapons, including nuclear ones, depend in their delivery on computer systems.

B. General introduction to Cybercrime: definitions and forms

a. Specific crimes: crimes related to the violation of copyrights and related rights

Violations of copyrights by the use of the computer and the internet pose a strong security obsession in light of the gravity of the assaults against data stored in the computers and the destruction and transfer of data, information, and ideas from databases and files of some governmental and non-governmental institutions. Hence, the courts in some countries deemed that data as chattels. This also has influenced the legislation developed to combat that type of crimes. For example, when preparing the Electronic Commerce Act in Luxemburg, the concept of chattel was broadened to embrace the crimes committed by use of computer against copyrights. The concept of writing in respect of forgery crimes was also changed so that it can be legally possible to prosecute an offender who commits a crime by using the computer.

Likewise, the American and French courts have broadened the concept of chattels as the use of computer and internet crimes have made it easy to assault databases. Therefore, both the American and French courts apply some existing provisions relative to assault against property to such activities, thus, raising controversy on whether those provisions apply to the suit in question. Another question is also raised: Does applying those provisions lead to a widening of the scope of law provisions, which goes in conflict with important and well-established principles in the criminal law such as the principles of the legality of crimes and punishment and their narrow interpretation?

b. Specific crimes: child and other pornography-related crimes

The wide spread of pornography on the internet has presently become an issue of international concern because of the huge increase of the users of the internet all over the world. Pornographic sites usually display different kinds and shapes of sex photos. These sites differ from the mailing lists through which sex photos and movies are exchanged. The purpose of these sites, usually, is to make profits. A browser of these sites has to pay a certain fee to watch a movie for a limited period of time or pay a monthly or annual subscription to benefit from the services of these sites, though some of these sites lure the user by sending some sex photos for free to their e-mail addresses daily.

These sites and lists have exploited the rapid spread of the internet and the other benefits it offers by using the best methods for distributing pornographic photos and movies publicly, thus, forcing their way into the people's houses and workplaces. One can find an unprecedented huge flood of pornographic photos, articles, and movies. The result is that every user of the net is prone to be influenced by that pornographic assault since it does not recognize any international or geographic borders. This, of course, poses a real danger to both children and adults in light of its harmful and undesired impacts.

C. Cyber legislation

Cybercrimes pose an extreme danger which has recently attracted the attention of governments and legislators. Though the legislations of most countries include provisions criminalizing these kinds of crimes and punishing their perpetrators, still these provisions are inoperative in most countries. For one reason, these crimes rapidly develop and spread. For another reason, there is a lack of experience on how to detect, trace, and gather evidence against these crimes.

At the international level, the United Nations Organization and most international and regional organizations attach special attention to this issue; a matter which resulted in a set of international standards. However, the international community still needs a binding international convention in this connection.

a. International instruments addressing these crimes

The Council of Europe's Cybercrime Convention of the year 2001 is the only multilateral convention concerned with combating cybercrimes. Since it has taken force in 1 July 2004 at the level of the member states of the Council of the European Union, the Convention represents the basic pillar in this respect⁷. As noted above, several non-member states signed this Convention also. These include Canada, Japan, and South Africa. The United States has already ratified the Convention and it took effect on 1 January 2007.

Meanwhile, the G-8 (group of 8 major industrialized nations) has also attached special attention to cybercrimes. The G-8 formed several action groups which issued many recommendations and decisions for prevention of this kind of crimes. Significant recommendations were issued by the so-called Lyon Group which was formed during the Halifax summit in Canada in 1995 under the name "Recommendations to Combat Transnational Organized Crime Efficiently"⁸. According to these recommendations:

States should review their laws in order to ensure that abuses of modern technology that are deserving of criminal sanctions are criminalized and that problems with respect to jurisdiction, enforcement powers, investigation, training, crime prevention and international cooperation in respect of such abuses are effectively addressed. Liaison between law enforcement and prosecution personnel of different States should be improved, including the sharing of experience in addressing these problems. States should promote study in this area and negotiate arrangements and agreements to address the problem of technological crime and investigation.

During the subsequent meetings of the G-8, several working groups were formed on technological crimes and many recommendations were issued. However, it is noted that the recommendations of these groups, of course, are not binding like the international conventions and standards. They are mere recommendations and guidelines.

At the level of the United Nations Organization, consultations are still underway concerning the formation of "a working group to curb cybercrime". The consultations took a serious shape following the first phase of the World Summit on Information Society (WSIS) which was held in Geneva late in December 2003 and discussed later

⁷ The full text of the cybercrime convention and more details on applying the convention exist on the EC electronic site. See:
- http://www.coe.int/t/el/legal_affairs/legal_co-operation/combating_economic_crime/6_Cybercrime
- <http://www.convention.coe.int/treaty/EN/treaties/htm/185.htm>

⁸ For further details on the activities of the G-8, see:
<http://www.g8.utoronto.ca/summit/1996lyon/index.htm>

in detail at the second phase of the summit which was held in Tunis late in November 2005. In that summit, the participating states agreed on the need to form the working group and formulate its objectives and relationships with the other organs.

b. Legislation in concerned Arab countries

Experiences in the Arab countries in the field of legislation for curbing cybercrime constitute no more than penal provisions in their penal codes addressing different crimes.

In Egypt, for example, Article 9 of Act 260/1980 concerning Civil Status amended by acts 11/1965 and 158/1980 provides that "the data contained in the civil status records are deemed confidential". The Memorandum of Law provides that "as these records contain the most accurate information about a person's status, this information is deemed confidential so that every one feels secure about the details he submits. The scope of confidentiality extends to cover anyone who is not authorized, under the Civil Status Act and its Executive Regulation and implementing decrees, to have an access to such information unless a judicial body or investigation authority issues a decision to have an access to or check such information. The reason for this is that a person's right to the privacy of his information is supported for the public interest. Being a secret, the disclosure of such information by an employee who is committed to keep it confidential, makes him punishable by Article 310 of the Penal Code".

Article 140 of Intellectual Property Protection Act 82/2002 also provides as follows:

"Protected by this Act, are the rights of authors in respect of their literary and art works, particularly, the following:

1.
2. computer programs.
3. Databases whether they are accessible from the computer or elsewhere."

The existing legislation in the other Arab countries is similar to that existing in the Arab Republic of Egypt. Arab positive legislations concerning cybercrimes are no more than some legislative provisions and penalties contained in the penal codes.

c. The elements that have to be addressed in national legislation

If we want to confront this new type of crime, there must be all-embracing, specific, deterrent and flexible national laws. These laws must contain the following elements:

1. A focus on the maintenance and respect of the privacy of individuals and groups against any violation.
2. A focus on achieving a balance between the protection of technology and the protection of individuals' rights.
3. A Specification of the different shapes of Cybercrime with an emphasis on the flexibility of laws so that other new forms and types of crimes can be added.
4. A focus on the importance of regional and international cooperation in the field of prevention, tracing, and prosecution of this type of crime in the light of the fact that they are by definition trans-national crimes of the first degree.

D. Building the capacity of human resources in the investigation, prosecution and trial of Cybercrime

a. Identify public prosecutors with advanced investigative techniques and methods of information gathering

A top priority of all initiatives for building the capacity of the national criminal systems to combat Cybercrime is the need to increase the judges' and public prosecutors' awareness about this type of serious crimes, mechanisms of their prevention, methods of investigation, and techniques for gathering information and evidence. The reason for this is that this type of crime is committed by computer and sometimes from a geographically distant country by using the internet. Therefore, it is difficult for the national law enforcement agencies to detect or trace them. It is also difficult to gather physical evidence to prove the committed crime. Hence, it is important to acquaint the public prosecutors with the new technologies used in detecting and investigating this type of crime and the ways to gather the physical technological evidence.

b. Identify public prosecutors with the methods of prosecution

It is very important to train the members of the law enforcement agencies, particularly the public prosecutors and investigation judges, on the means to confront this type of crime which is committed away from the eyes of the law enforcement agencies. This training must include introducing the public prosecutors to the modern techniques of prosecuting this type of crime and the ways to use them so that the perpetrators of these crimes can be brought to justice.

c. The role of public prosecutors in evaluating cybercrime evidence – proof system

The public prosecution institution is the authority responsible for investigating these crimes in general. Hence, it is the body which gathers and evaluates the physical evidence of the crime before it remits the case to the criminal court. Therefore, it is important to increase the abilities of the public prosecutors and train them on how to monitor and evaluate the technological physical evidence. However, this depends in the first place on the national procedural laws in such a way that conforms to the requirements of the present age and the threats that technology and scientific progress impose.

d. Build the technical capacity of the public prosecutors to inspect the Cybercrime scene

A major element of the criminal investigation assumed by the public prosecution institution is the inspection of the crime scene and establishing its elements and crime traces. This, of course, relates to the ordinary concept of the crime scene; namely, the physical place at which the crime was committed. However, the situation here is different. This is because cybercrime is committed by computer and perhaps in another country by using the internet. Thus, crime scene inspection requires the use of

advanced technological techniques, special training, and a high degree of knowledge. All these issues will be addressed in the workshop.

5. Preventive measures and international cooperation to combat Cybercrime

a. The role of cooperation between the public and private sectors in addressing Cybercrime

Cybercrime has become a part of our daily life as it spreads rapidly and easily across the international borders. The first victim here is the ordinary user of the computer being a child or an old man, a small firm or an international company, or even a government. Therefore, cooperation and partnership between the public and private sectors in confronting these crimes is no longer a choice but, rather, an inevitability to put an end to the serious spread of cybercrime.

This cooperation is the most effective mechanism for preventing the perpetrators of these crimes from evading punishment. It also supports other efforts in this field. Therefore, both the public and private sectors should reach an agreement on the standards of this cooperation, mechanisms for its activation, and methods of its confrontation, and exchange of experiences.

b. The importance of international cooperation in exchanging information and methods of investigation

International cooperation is the first block and mainstay in combating these types of crimes as they are often committed in different parts of the world by using modern technologies. The need for international cooperation was stressed by the Council of Europe's Cybercrime Convention when it called on the member states to cooperate in extradition and mutual assistance in investigation and evidence gathering, and take the necessary legislative measures that would enable them to meet these obligations.

The Arab region, in its turn, is in dire need for establishing and consolidating mechanisms for cooperation among the region's countries to combat this type of crimes which has pervaded the Arab region particularly in the absence of special laws governing them. It is worth noting that the list of the countries classified as "countries with effective and advanced laws" does not include any Arab country.

c. Promote channels of communication between countries by designating contacts in each country

To strengthen cooperation between countries, there should be certain offices and persons serving as contacts and focal points between the different countries. Admittedly, there are urgent cases and other cases where swift action is crucial. Therefore, the presence of these offices and persons conferred to take decisions helps investigate and track down these crimes.

6. Co-sponsors; venue and date:

- The regional conference will be held in cooperation between the United Nations Development Programme – Program for Governance in the Arab Region (UNDP-POGAR) and the Ministry of Justice in the Kingdom of Morocco.
- The Council of Europe contributed in organizing this conference by assisting the Project's Management Team in preparing the conference's program and by providing the Project with four experts to give presentations and benefit the participants with their wide experience in the cybercrime field.
- The conference will be held in Royal Mansour Meridien Hotel, Casablanca. Tel: 00212- 2- 231 3011.
- The conference will open at 9.00 am on Tuesday 19 June 2007 and continue for one and half days.