**El Hassan Yahya, Legal Expert with the League of Arab States**
**Rabat, Morocco**

## Session III: Special Investigation Techniques, the Internet and Telecommunications

Consolidated report

We should first of all point out that Session III on Special Investigation Techniques, Internet and Telecommunications was highly "technical" in content. Thanks to the nature of the subject addressed and the quality of the individual speakers, who are experts in the field of cybernetic investigations and computer system processing, a number of basic principles were highlighted:

1) "Cyberspace" is in a permanent state of flux, so much so that the burgeoning power of the Internet inevitably leads to adverse developments which can trigger constantly evolving cross-border cybercrime.

2) "Cyberspace", which displays specific features that contrast starkly with those of the real world, sometimes calls for different investigation techniques which are more suitable than those which are traditionally used.

Existing legislation cannot be adapted to the new technologies in real time. The formalism of certain rules of procedure reinforces the impression that the legal framework is unsuited to actual practice.

This means that we need a legal framework for authorising investigatory methods which would allow investigators to carry out their investigations properly.

3) It is difficult to intercept exchanges via Internet, and indeed it is impossible via the technical methods of phone-tapping. The example of the Skype system was mentioned.

4) Cybercrime infringes the traditional principle of territoriality of criminal law, since offences can be committed simultaneously in several different countries. A number of difficulties can seriously hamper investigations if we scrupulously apply the concept of national sovereignty. Similarly, the introduction of new digital systems for outsourcing data on to virtual servers, such as "cloud computing", could cause innumerable difficulties which must be overcome if we are to establish the basic rules for territorial jurisdiction.

5) The increasing number of websites being used as tools for propaganda and recruitment for terrorist purposes, their global accessibility and the volume of information circulating in them are tending to complicate surveillance activities, even more so when Internet users are anonymous or use borrowed names.

The speakers unequivocally considered that this highlights the vital need for special investigation techniques. This requirement is in line with the radical changes which have been affecting modern societies for the past two decades, the symptoms of which might be described as follows:

- internationalisation of criminal law under the influence of globalisation;

- the inability of legal systems to manage mass litigation in accordance with the "conventional" responses of criminal law;

- police pressure to obtain more effective investigatory resources;

- the emergence of a "surveillance society".

This "postmodern criminal law" phenomenon as described by Professor Michel Massé (*Un droit pénal postmoderne?* Publ. PUF/2009, pp. 24 and 25) emerged with the "terrorist threat", which, under the effect of the panic which it causes, intensified the swing in western societies from a "democracy of opinion" to a "democracy of emotion", whereby the very principles of criminal law systems give way to "emergency legislation".

The aim of this legislation is not to punish an act or sanction a person, but rather to "prevent risks".

It is within this preventive framework that we can conceive the legal possibility of implementing special investigation techniques via "exceptional" legal restrictions on human rights and fundamental freedoms.

The requisite balance between action against terrorism and organised crime on the one hand and respect for human rights on the other involves establishing an order of priority in norms and values, in terms of both preparing and implementing legislation. It must be borne in mind that both these apparently contradictory objectives promote the concept of equitable justice.

I would like to present the following recommendations in order to help achieve this balance:

I) Creating a body of procedural legislation explicitly authorising recourse to special investigation techniques. Under no circumstances must these techniques be placed on an equal footing with the conventional rules of criminal procedural law.

The scope of this equality principle must be clearly delimited, with a view to protecting the individual against arbitrary interference by the public authorities.

II) Harmonising national legislations with a set of international principles regulating the modes of application of special investigation techniques, serving as a common language for international co-operation.

The lack of a clear, uniform and internationally recognised definition of terrorism will make it difficult to secure an international delimitation of the scope of special investigation techniques.

III) Relaxing the binding rules of the national sovereignty principle by authorising the setting up of joint investigation groups. These groups will be mandated to work simultaneously on the same case in order to offset the problems vis-à-vis the territoriality principle caused by transfrontier cybercrime and the volatility of computer files.

It is in the public interest in such cases to create an atmosphere of mutual trust and to encourage personal contacts between the various government departments belonging to the different regional and international groups.

IV) Reinforcing the role of judges in implementing special investigation techniques with a view to highlighting the end of the work of the intelligence service and the beginning of the judicial investigations, given that the boundary between these two departments is fairly vague, or even non-existent in some cases.

Using such special investigation techniques, which formerly fell within the exclusive jurisdiction of the intelligence field, and placing them under judicial supervision, will not lead to the legalisation of the work of the intelligence services.

V) Extending the training of judges to embrace technical skills for appraising, with full knowledge of the facts, the legality of the investigation methods envisaged and supervising their implementation. This is necessary in order to verify the compatibility of such measures with human rights.

It must be pointed out that the whole area of digital technology is a matter of concern for lawyers, many of whom have scant knowledge of the technical aspects, even though such knowledge is necessary for the implementation of high-quality justice and a fair trial.

VI) Enhancing the partnership between the public and private sectors, given that the latter has the necessary data for establishing digital evidence, both in terms of technology and expertise.

It is vital to ensure such co-operation at a time when new practices are developing in such a way as to deprive investigatory agencies of the necessary investigatory resources unless they maintain constructive relations with the private sector.

It is essential to co-ordinate the efforts of governmental and non-governmental agencies in combating such crime, which is geared to destabilising modern societies and eliminating their democratic values.