Workshop on

# "RACIST AND XENOPHOBIC CONTENT ON THE INTERNET – PROBLEMS AND SOLUTIONS"

Düsseldorf, 31 October 2002

by Gianluca Esposito, Directorate General I – Legal Affairs, Council of Europe1

## I. Introduction

I am grateful to the organisers for the opportunity of presenting today – for the first time after its approval by the 44 Ministers' Deputies of the Council of Europe – the Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems. This Additional Protocol has been adopted by the Committee of Ministers of Foreign Affairs on 7 November 2002 and will be open to signature in January 2003.

## II. Background

Since the adoption in 1948 of the Universal Declaration of Human Rights, the international community has made important progress in the fight against racism, racial discrimination, xenophobia and related intolerance. National and international laws have been enacted and a number of international human rights instruments have been adopted, in particular, the International Convention of New York of 1966 on the Elimination of All Forms of Racial Discrimination, concluded in the framework of the United Nations needs to be mentioned (CERD). Although progress has been made, yet, the desire for a world free of racial hatred and bias remains only partly fulfilled.

As technological, commercial and economic developments bring the peoples of the world closer together, racial discrimination, xenophobia and other forms of intolerance continue to exist in our societies. Globalisation carries risks that can lead to exclusion and increased inequality, very often along racial and ethnic lines.

[1] The opinions expressed in this paper are those of the author and do not necessarily reflect those of the Council of Europe.

In particular, the emergence of international communication networks like the Internet provide certain persons with modern and powerful means to support racism and xenophobia and enables them to disseminate easily and widely expressions containing such ideas. In order to investigate and prosecute such persons, international co-operation is vital. The Convention on Cybercrime (ETS 185) was drafted to enable mutual assistance concerning computer related crimes in the broadest sense in a flexible and modern way.

The Convention on cybercrime, one of the major achievements of the more than 50 year long Council of Europe treaty-making tradition, which was opened to signature in Budapest on 23 November 2001 and so far signed by 34 European and non-European States and ratified by 1 State (Albania), has received strong support from law-makers and practitioners throughout Europe and beyond.

However, I will not hide from you that the Convention has also been criticised on various grounds by a number of associations, particularly those active in the protection of freedom of expression, and also by representatives of certain branches of industry. So has the Additional Protocol. However, I must say that I do not share most of the criticism made to these texts and not for merely "unilateral" views.

The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future.

These developments have given rise to unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies.

The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The Convention on cybercrime and its Additional Protocol aim to meet this challenge, with due respect to human rights in the new Information Society. Both texts contain provisions concerning the following offences:

- Computer-related offences: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related forgery, computer-related fraud.

- Content-related offences: child pornography (Art. 9 of the Convention on cybercrime) and racism and xenophobia on the Internet.

The committee drafting the Convention discussed the possibility of including other content-related offences, such as the distribution of racist propaganda through computer systems. However, the committee was not in a position to reach consensus on the criminalisation of such conduct. While there was significant support in favour of including this as a criminal offence, some delegations expressed strong concern about including such a provision on freedom of expression grounds. Noting the complexity of the issue, it was decided that the committee would refer to the European Committee on Crime Problems (CDPC) the issue of drawing up an additional Protocol to the Convention.

The Parliamentary Assembly, in its Opinion 226(2001) concerning the Convention, recommended immediately drawing up a protocol to the Convention under the title "Broadening the scope of the convention to include new forms of offence", with the purpose of defining and criminalising, inter alia, the dissemination of racist propaganda.

The Committee of Ministers therefore entrusted the European Committee on Crime Problems (CDPC) and, in particular, its Committee of Experts on the Criminalisation of Acts of a Racist and xenophobic Nature committed through Computer Systems (PC-RX), with the task of preparing a draft additional Protocol, a binding legal instrument open to the signature and ratification of Contracting Parties to the Convention, dealing in particular with the following:

i. the definition and scope of elements for the criminalisation of acts of a racist and xenophobic nature committed through computer networks, including the production, offering, dissemination or other forms of distribution of materials or messages with such content through computer networks;

ii. the extent of the application of substantive, procedural and international co-operation provisions in the Convention on Cybercrime to the investigation and prosecution of the offences to be defined under the additional Protocol.

## III. The Additional Protocol

### A. Aims

The purpose of this Protocol is twofold: firstly, harmonising substantive criminal law in the fight against racism and xenophobia on the Internet and, secondly, improving international co-operation in this area. This kind of harmonisation alleviates the fight against such crimes on the national and on the international level. Corresponding offences in domestic laws may prevent misuse of computer systems for a racist purpose by Parties whose laws in this area are less well defined. As a consequence, the exchange of useful common experiences in the practical handling of cases may be enhanced too. International co-operation (especially extradition and mutual legal assistance) is facilitated, e.g. regarding requirements of double criminality.

### B. Structure

The Additional Protocol contains four chapters: (I) Common provisions (containing in particular the definition of "racist and xenophobic material"), (II) Measures to be taken at a national level – substantive law, (III) Relationship between the Convention and the Additional Protocol and (IV) Final clauses.

### C. Common provisions

This part of the Additional Protocol contains a definition of racist and xenophobic material. It refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, of a racist and xenophobic nature, in such a format that it can be stored, processed and transmitted by means of a computer system. The definition contained in Article 2 of this Protocol refers to certain conduct to which the content of the material may lead, rather than to the expression of feelings/belief/aversion as contained in the material concerned. The definition builds upon existing national and international (UN, EU) definitions and documents as far as possible.

Several legal instruments have been elaborated at an international and national level to combat racism or xenophobia. The drafters of this Protocol took account in particular of (i) the

International Convention on the Elimination of All Forms of Racial Discrimination (CERD), (ii) Protocol No. 12 (ETS 177) to the Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), (iii) the Joint Action of 15 July 1996 of the European Union adopted by the Council on the basis of Article K.3 of the Treaty on the European Union, concerning action to combat racism and xenophobia, (iv) the World Conference against Racism, Racial Discrimination, Xenophobia and Related Intolerance (Durban, 31 August-8 September 2001), (v) the conclusions of the European Conference against racism (Strasbourg, 13 October 2000) (vi) the comprehensive study published by the Council of Europe Commission against Racism and Xenophobia (ECRI) published in August 2000 (CRI(2000)27) and (vii) the November 2001 Proposal by the European Commission for a Council Framework Decision on combating racism and xenophobia (in the framework of the European Union).

Article 10 of the ECHR recognises the right to freedom of expression, which includes the freedom to hold opinions and to receive and impart information and ideas. "Article 10 of the ECHR is applicable not only to information and ideas that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb the State or any sector of the population"2. However, the European Court of Human Rights held that the State's actions to restrict the right to freedom of expression were properly justified under the restrictions of paragraph 2 of Article 10 of the ECHR, in particular when such ideas or expressions violated the rights of others. This Protocol, on the basis of national and international instruments, establishes the extent to which the dissemination of racist and xenophobic expressions and ideas violates the rights of others.

The definition contained in Article 2 refers to written material (e.g. texts, books, magazines, statements, messages, etc.), images (e.g. pictures, photos, drawings, etc.) or any other representation of thoughts or theories, of a racist and xenophobic nature, in such a format that it can be stored, processed and transmitted by means of a computer system.

The definition contained in Article 2 of this Protocol refers to certain conduct to which the content of the material may lead, rather than to the expression of feelings/belief/aversion as contained in the material concerned. The definition builds upon existing national and international (UN, EU) definitions and documents as far as possible.

The definition requires that such material advocates, promotes, incites hatred, discrimination or violence. "Advocates" refers to a plea in favour of hatred, discrimination or violence, "promotes" refers to an encouragement to or advancing hatred, discrimination or violence and "incites" refers to urging others to hatred, discrimination or violence.

[2] See in this context, for instance, the Handyside judgment of 7 December 1976, Series A, no. 24, p. 23, para. 49.

The term "violence" refers to the unlawful use of force, while the term "hatred" refers to intense dislike or enmity.

When interpreting the term "discrimination", account should be taken of the ECHR (Article 14 and Protocol 12), and of the relevant case-law, as well as of Article 1 of the CERD. The prohibition of discrimination contained in the ECHR guarantees to everyone within the jurisdiction of a State Party equality in the enjoyment of the rights and freedoms protected by the ECHR itself. Article 14 of the ECHR provides for a general obligation for States, accessory to the rights and freedoms provided for by the ECHR. In this context, the term "discrimination" used in the Protocol refers to a different unjustified treatment given to persons or to a group of persons on the basis of certain characteristics. In the several judgments (such as the Belgian Linguistic case, the Abdulaziz, Cabales and Balkandali judgment3) the European Court of Human Rights stated that "a difference of treatment is discriminatory if it 'has no objective and reasonable justification', that is, if it does not pursue a 'legitimate aim' or if there is not a 'reasonable relationship of proportionality between the means employed and the aim sought to be realised'". Whether the treatment is discriminatory or not has to be considered in the light of the specific circumstances of the case. Guidance for interpreting the term "discrimination" can also be found in Article 1 of the CERD, where the term "racial discrimination" means "any distinction, exclusion, restriction or preference based on race, colour, descent, or national or ethnic origin which has the purpose or effect of nullifying or impairing the recognition, enjoyment or exercise, on an equal footing, of human rights and fundamental freedoms in the political, economic, social, cultural or any other field of public life".

Hatred, discrimination or violence, have to be directed against any individual or group of individuals, for the reason that they belong to a group distinguished by "race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors".

It should be noted that these grounds are not exactly the same as the grounds contained, for instance, in Article 1 of Protocol No. 12 to the ECHR, as some of those contained in the latter are alien to the concept of racism or xenophobia. The grounds contained in Article 2 of this Protocol are also not identical to those contained in the CERD, as the latter deals with "racial discrimination" in general and not "racism" as such. In general, these grounds are to be interpreted within their meaning in established national and international law and

[3] Abulaziz, Cabales and Balkandali, judgment of 28 May 1985, Series A no. 94, p. 32, para. 62; Belgian Linguistic case, judgment of 23 July 1968, Series A no. 6, p. 34, para. 10.

practice. However, some of them require further explanation as to their specific meaning in the context of this Protocol.

"Descent" refers mainly to persons or groups of persons who descend from persons who could be identified by certain characteristics (such as race or colour), but not necessarily all of these characteristics still exist. In spite of that, because of their descent, such persons or groups of persons may be subject to hatred, discrimination or violence. "Descent" does not refer to social origin.

The notion of "national origin" is to be understood in a broad factual sense. It may refer to individuals' histories, not only with regard to the nationality or origin of their ancestors but also to their own national belonging, irrespective of whether from a legal point of view they still possess it. When persons possess more than one nationality or are stateless, the broad interpretation of this notion intends to protect them if they are discriminated on any of these grounds. Moreover, the notion of "national origin" may not only refer to the belonging to one of the countries that is internationally recognised as such, but also to minorities or other groups of persons, with similar characteristics.

The notion of "religion" often occurs in international instruments and national legislation. The term refers to conviction and beliefs. The inclusion of this term as such in the definition would carry the risk of going beyond the ambit of this Protocol. However, religion may be used as a pretext, an alibi or a substitute for other factors, enumerated in the definition. "Religion" should therefore be interpreted in this restricted sense.

A specificity of the offences included is the express requirement that the conduct involved is done "without right". It reflects the insight that the conduct described is not always punishable per se, but may be legal or justified not only in cases where classical legal defences are applicable, like consent, self defence or necessity, but where other principles or interests lead to the exclusion of criminal liability (e.g. for law enforcement purposes, for academic or research purposes). The Protocol, therefore, leaves unaffected conduct undertaken pursuant to lawful government authority (for example, where the Party's government acts to maintain public order, protect national security or investigate criminal offences).

Moreover, all the offences contained in the Protocol must be committed "intentionally" for criminal liability to apply. In certain cases an additional specific intentional element forms part of the offence. The drafters of the Protocol, as those of the Convention, agreed that the exact meaning of 'intentionally' should be left to national interpretation. Persons cannot be held criminally liable for any of the offences in this Protocol, if they have not the

required intent. It is not sufficient, for example, for a service provider to be held criminally liable under this provision, that such a service provider served as a conduit for, or hosted a website or newsroom containing such material, without the required intent under domestic law in the particular case. Moreover, a service provider is not required to monitor conduct to avoid criminal liability.

D. Criminal offences

The Additional Protocol contains the following offences:

- Dissemination of racist and xenophobic material through computer systems,
- Racist and xenophobic motivated threat,
- Racist and xenophobic motivated insult,
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity,
- Aiding and abetting any of the offences contained in the Protocol.

Dissemination of racist and xenophobic material through computer systems: this Article requires States Parties to criminalize distributing or otherwise making available racist and xenophobic material to the public through a computer system. The act of distributing or making available is only criminal if the intent is also directed to the racist and xenophobic character of the material.

The term "to the public" used in Article 3 makes it clear that private communications or expressions communicated or transmitted through a computer system fall outside the scope of this provision. Indeed, such communications or expressions, like traditional forms of correspondence, are protected by Article 8 of the ECHR.

Whether a communication of racist and xenophobic material is considered as a private communication or as a dissemination to the public, has to be determined on the basis of the circumstances of the case. Primarily, what counts is the intent of the sender that the message concerned will only be received by the pre-determined receiver. The presence of this subjective intent can be established on the basis of a number of objective factors, such as the content of the message, the technology used, applied security measures, and the context in which the message is sent. Where such messages are sent at the same time to more than one

recipient, the number of the receivers and the nature of the relationship between the sender and the receiver/s is a factor to determine whether such a communication may be considered as private.

Exchanging racist and xenophobic material in chat rooms, posting similar messages in newsgroups or discussion fora, are examples of making such material available to the public. In these cases the material is accessible to any person. Even when access to the material would require authorisation by means of a password, the material is accessible to the public where such authorisation would be given to anyone or to any person who meets certain criteria. In order to determine whether the making available or distributing was to the public or not, the nature of the relationship between the persons concerned should be taken into account.

Racist and xenophobic motivated threat: Most legislation provide for the criminalisation of threat in general. The drafters agreed to stress in the Protocol that, beyond any doubt, threats for racist and xenophobic motives are to be criminalized.

The notion of "threat" may refer to a menace which creates fear in the persons to whom the menace is directed, that they will suffer the commission of a serious criminal offence (e.g. affecting the life, personal security or integrity, serious damage to properties, etc., of the victim or their relatives). It is left to the States Parties to determine what is a serious criminal offence.

According to this Article, the threat has to be addressed either to (i) a person for the reason that he or she belongs to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or to (ii) a group of persons which is distinguished by any of these characteristics. There is a no restriction that the threat should be public. This Article also covers threats by private communications.

Racist and xenophobic motivated insult: Article 5 deals with the question of insulting publicly a person or a group of persons because they belong or are thought to belong to a group distinguished by specific characteristics. The notion of "insult" refers to any offensive, contemptuous or invective expression which prejudices the honour or the dignity of a person. It should be clear from the expression itself that the insult is directly connected with the insulted person's belonging to the group. Unlike in the case of threat, an insult expressed in private communications is not covered by this provision.

Denial, gross minimisation, approval or justification of genocide or crimes against humanity: In recent years, various cases have been dealt with by national courts where persons (in public, in the media, etc.) have expressed ideas or theories which aim at denying, grossly minimising, approving or justifying the serious crimes which occurred in particular during the second World War (in particular the Holocaust). The motivation for such behaviours is often presented with the pretext of scientific research, while they really aim at supporting and promoting the political motivation which gave rise to the Holocaust. Moreover, these behaviours have also inspired or, even, stimulated and encouraged, racist and xenophobic groups in their action, including through computer systems. The expression of such ideas insults (the memory of) those persons who have been victims of such evil, as well as their relatives. Finally, it threatens the dignity of the human community.

Article 6, which has a similar structure as Article 3, addresses this problem. The drafters agreed that it was important to criminalize expressions which deny, grossly minimise, approve or justify acts constituting genocide or crimes against humanity, as defined by international law and recognised as such by final and binding decisions of the International Military Tribunal, established by the London Agreement of 8 April 1945. This owing to the fact that the most important and established conducts, which had given rise to genocide and crimes against humanity, occurred during the period 1940-1945. However, the drafters recognised that, since then, other cases of genocide and crimes against humanity occurred, which were strongly motivated by theories and ideas of a racist and xenophobic nature. Therefore, the drafters considered it necessary not to limit the scope of this provision only to the crimes committed by the Nazi regime during the 2nd World War and established as such by the Nuremberg Tribunal, but also to genocides and crimes against humanity established by other international courts set up since 1945 by relevant international legal instruments (such as UN Security Council Resolutions, multilateral treaties, etc.). Such courts may be, for instance, the International Criminal Tribunals for the former Yugoslavia, for Rwanda, the Permanent International Criminal Court. This Article allows to refer to final and binding decisions of future international courts, to the extent that the jurisdiction of such a court is recognised by the Party signatory to this Protocol.

The provision is intended to make it clear that facts of which the historical correctness has been established may not be denied, grossly minimised, approved or justified in order to support these detestable theories and ideas.

The European Court of Human Rights has made it clear that the denial or revision of "clearly established historical facts – such as the Holocaust – […] would be removed from

the protection of Article 10 by Article 17" of the ECHR (see in this context the Lehideux and Isorni judgment of 23 September 1998)[4].

Aiding and abetting: The purpose of this article is to establish as criminal offences aiding or abetting the commission of any of the offences under the Protocol. Contrary to the Convention, the Protocol does not contain the criminalisation of the attempt to commit the offences contained in it, as many of the criminalized conducts have a preparatory nature.

Liability arises for aiding or abetting where the person who commits a crime established in the Protocol is aided by another person who also intends that the crime be committed. For example, although the transmission of racist and xenophobic material through the Internet requires the assistance of service providers as a conduit, a service provider that does not have the criminal intent cannot incur liability under this section. Thus, there is no duty on a service provider to actively monitor content to avoid criminal liability under this provision.

As with all the offences established in accordance with the Protocol, aiding or abetting must be committed intentionally.

E. Procedural powers, jurisdiction and international co-operation

The provisions of the Convention concerning the above matters apply or have to be extended, as the case may be, to the Additional Protocol.

Procedural powers: the provisions of the Convention, which States are required to extend to the offences contained in the Protocol as well, seek to establish common rules concerning procedural powers, either by adapting some traditional procedural measures, such as search and seizure, to the new technological environment or by creating new measures, such as expedited preservation of data, in order to ensure that traditional measures of collection, such as search and seizure, remain effective in the volatile technological environment. As data in the new technological environment is not always static, but may be flowing in the process of communication, other traditional collection procedures relevant to telecommunications, such as real-time collection of traffic data and interception of content data, have also been adapted in order to permit the collection of electronic data that is in the process of communication.

[4] Lehideux and Isorni judgment of 23 September 1998, Reports 1998-VII, para. 47.

The use of these procedures will make it possible to find and gather electronic evidence, relating to both the offences set out in the Convention (e.g. child pornography) and other offences (e.g. money laundering). The procedural-law section is therefore broader in scope than the substantive-law section: it will be possible to use the different types of investigative powers in cases where an offence is committed by means of a computer system or in which evidence of a crime is electronic.

The text concerns only specific criminal investigations and cannot be used, as some people seem to suspect, to set up a widespread "Orwellian" system of electronic surveillance. It will undeniably make it possible to seize data, or to oblige the person who possesses the data in question to disclose it, or to preserve data for the purposes of the investigation, but the Convention does not require and cannot justify the surveillance of personal communications or contacts by either service providers or law enforcement agencies, unless there is an official criminal investigation. All these provisions aim at permitting the obtaining or collection of data for the purpose of specific criminal investigations or proceedings. The drafters of the Convention discussed whether the Convention should impose an obligation for service providers to routinely collect and retain traffic data for a certain fixed period of time, but did not include any such obligation due to lack of consensus.

In addition, the drafters have included a large number of procedural guarantees, which will make it possible to prevent any abuse of the procedures it defines. First of all, the text spells out that the introduction, implementation and application of the powers and procedures set out in the Convention will be subject to the conditions and safeguards provided for by the domestic law of each Party, having regard to the need for adequate human rights protection, especially as defined in the relevant international instruments (in particular the ECHR and the International Covenant on Civil and Political Rights). It also advocates that, before applying the measures envisaged, future Contracting states should ensure that these are proportional to the nature of and circumstances surrounding the offence under investigation. Finally, the text stipulates, with regard to each procedure, that the relevant domestic conditions and safeguards must be applied; contracting states will therefore be required to apply existing safeguards to investigations, for example, making them conditional on authorisation from a judge or minister, depending on the country concerned. It should also be realised that it would have been impossible to harmonise these procedural safeguards, if only at European level. However, these safeguards do exist in the member states' domestic law and are supposed to provide a similar level of human rights protection throughout the continent.

The convention deals with the following powers:

1. expedited preservation of stored computer data;
2. expedited preservation and partial disclosure of traffic data;
3. production order;
4. search of computer systems;
5. seizure of stored computer data;
6. real-time collection of traffic data;
7. interception of content data.

International Co-operation: This part of the Convention, which States are required to extend to the provisions contained in the Protocol as well, is, in the eyes of many, the most important, as it makes it possible to implement the rapid and effective co-operation required in investigations into computer-related crimes. Where electronic evidence - which is very volatile by nature - is concerned, it is essential that law-enforcement agencies should be able to carry out investigations on behalf of other states, and pass on the information with greater rapidity. In addition to traditional forms of international co-operation on crime (mutual assistance and extradition) the convention stipulates that Contracting states should apply the procedures set out in the preceding part of the Convention as new forms of mutual assistance (for example the seizure or preservation of data on behalf of another Party). Clearly, one of the fundamental objectives of the convention is to enable the application of common computer-crime specific procedural powers at an international level, through a range of cooperation channels, including existing mutual assistance arrangements and also new avenues (the 24/7 network).

The Convention makes clear that international cooperation is to be provided among contracting states "to the widest extent possible." This principle requires them to provide extensive cooperation to each other, and to minimize impediments to the smooth and rapid flow of information and evidence internationally. The general scope of the obligation to cooperate stems from that of the procedural powers defined by the treaty: cooperation is to be provided in relation to the offences established by it, as well as all to criminal offences related to computer systems and data and to the collection of evidence in electronic form of a criminal offence. This means that either where the crime is committed by use of a computer system, or where an ordinary crime not committed by use of a computer system (e.g., a murder) involves electronic evidence, the convention is applicable.

The Convention also creates the legal basis for an international computer crime-specific assistance network, a network of national contact points available on a permanent basis ("24/7

network"). As has been previously discussed, effective combating of crimes committed by use of computer systems and effective collection of evidence in electronic form requires very rapid response. Moreover, with a few keystrokes, action may be taken in one part of the world that instantly has consequences many thousands of kilometres and many time zones away. For this reason, existing police cooperation and mutual assistance modalities require supplemental channels to address the challenges of the computer age effectively. The channel established in the convention is based upon the experience gained from an already functioning network created under the auspices of the G8 group of nations. Under the convention, each Party has the obligation to designate a point of contact available 24 hours per day, 7 days per week in order to ensure immediate assistance in investigations and proceedings within the scope of the convention. The establishment of this network is among the most important means provided by the convention of ensuring that contracting states can respond effectively to the law enforcement challenges posed by computer- crime. This network will not replace but supplement the more traditional channels of cooperation.

Each national 24/7 point of contact is to either facilitate or directly carry out, inter alia, the providing of technical advice, preservation of data, collection of evidence, giving of legal information, and locating of suspects. States can determine where to locate the point of contact within its law enforcement structure: some may wish to house the 24/7 contact within the central authority for mutual assistance, some may believe that the best location is with a police unit specialized in fighting computer-crime. Since the 24/7 contact is to provide both technical advice for stopping or tracing an attack, as well as such international cooperation duties as locating of suspects, there is no one correct answer, and it is anticipated that the structure of the network will evolve over time. The convention provides among the critical tasks to be carried out by the 24/7 contact the ability to facilitate the rapid execution of measures if it does not carry them out directly itself. For example, if a Party's 24/7 contact is part of a police unit, it must have the ability to coordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance, in order that appropriate action may be taken at any hour of the day or night. Moreover, 24/7 contacts must have the capacity to carry out communications with other members of the network on an expedited basis and have proper equipment. Up-to-date telephone, fax and computer equipment will be essential to the smooth operation of the network, and other forms of communication and analytical equipment will need to be part of the system as technology advances. The convention also requires that personnel participating as part of a national team for the network be properly trained regarding computer- or computer-related crime and how to respond to it effectively.

Finally, it has to be noted with respect to international cooperation that there are no plans, at this stage, for genuine cross-border investigations, such as cross-border searches into computer systems, because the negotiating states were unable to agree on such arrangements.

Jurisdiction: Amongst the various important issues addressed by the Convention and which apply to the Protocol as well, there is certainly the question of jurisdiction in relation to information technology offences, e.g. to determine the place where the offence was committed (locus delicti) and which law should accordingly apply, including the problem of ne bis idem in the case of multiple jurisdictions and the question how to solve positive jurisdiction conflicts and how to avoid negative jurisdiction conflicts.

This provision establishes a series of criteria under which Contracting Parties are obliged to establish jurisdiction over the criminal offences enumerated in Articles 2-11 of the Convention.

To deter and punish domestic crimes, States must have the ability to investigate and prosecute crimes established by the Convention that are committed in its territory and paragraph 1 littera a, which is based upon the principle of territoriality, requires States to do so.

The majority of States participating in the negotiations also recognised jurisdiction over cybercrime committed extraterritorially in certain cases, ie. over their nationals or if the crime is committed on a boat or a plane that they had registered and paragraphs 1b.c.d require jurisdiction to be established for these cases as well, with a full or partial reservation possibility for those States whose legal system does not allow application of these principles of extraterritorial scope.

This provision also requires States exercising jurisdiction to coordinate their efforts in appropriate cases, eg. when the targeted victims are located in different countries. In this case, co-ordination of such investigation and prosecution is vital to maximise the effectiveness of the fight against cybercrime.

## IV. Conclusion

It is clear that global threats and challenges need global responses. For this reason, the fight against cybercrime in general and racist and xenophobia on the Internet in particular, is carried out within the Council of Europe involving some non-European States in the negotiations process and opening the resulting treaties to their signature. As a consequence, the USA, Mexico, Japan, Canada and South-Africa have signed the Cybecrime Convention and are likely to sign also the Additional Protocol.

The www is a new world. A world in which relationships between individuals take place and on and through which crimes are committed. Self-regulation is, unfortunately, not enough. The Council of Europe, which has been protecting for more than 50 years in the real world, individuals' rights and freedoms through its European Court of Human Rights, seeks to protect the same rights and freedoms mutatis mutandis in the virtual world with certain safeguards. This is all the Additional Protocol does: it establishes the extent to which the

dissemination of racist and xenophobic expressions and ideas violates the rights of others and criminalises accordingly certain conducts.

Finally, there needs to be closer co-operation between law-enforcement authorities and ISPs, within an internationally agreed legal framework: I am convinced that the new Council of Europe Protocol provides for such a framework.