COUNCIL OF EUROPE CONSEIL DE L'EUROPE

T-CY (2008) 04

Strasbourg, 8 April 2008

THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

3nd Multilateral Consultation of the Parties to the Convention on cybercrime [ETS No 185]

Strasbourg, 3 and 4 April 2008

MEETING REPORT[1]

BRIEF FOREWORD

The T-CY welcomed the growing and widespread international support for the Convention on Cybercrime and invited those States which had not already done so to become Parties as soon as possible.

It underlined the important achievements of the Project on cybercrime and in particular took note of the non-binding Guidelines adopted by the Octopus Interface Conference on co-operation against cybercrime concerning "co-operation between law enforcement and Internet service providers in the investigation of cybercrime."

The T-CY made a number of proposals to facilitate the implementation of the Convention and, in particular, requested States to provide, where they had not already done so, information concerning points of contact for the 24/7 network, translations of the Convention and country profiles.

The T-CY also took note of certain international instruments relevant to cybercrime, the work of certain committees and the Internet Governance Forum (IGF).

[1] For further information concerning the T-CY and the Project on cybercrime please see: www.coe.int/cybercrime

TABLE OF CONTENTS

REPORT

I. INTRODUCTION

1. The Cybercrime Convention Committee (T-CY) met in G Building, Council of Europe, Strasbourg on 3 and 4 April 2008. This meeting took place within the framework of Article 46 of the Convention on Cybercrime [ETS No 185] (hereafter "the Convention") which provides that "The Parties shall, as appropriate, consult periodically …" .

2. The T-CY was opened by Ms Margaret KILLERBY (Secretary a.i. to the T-CY) who welcomed the participants to the 3rd meeting of the Parties.

3. The list of participants and the agenda, which refers to the documents for each agenda item, appear in **Appendices I and II** respectively.

4. The T-CY warmly thanked the outgoing Chair, Mr Henrik KASPERSEN (Netherlands), for his major contribution to the work of the Council of Europe in the field of cybercrime and in particular for chairing both the T-CY and the Committee of experts which prepared the Convention.

5. Ms Betty SHAVE (United States) was elected Chair and Ms Cristina SCHULMAN (Romania) was elected Vice-Chair by the States Party to the Convention.

6. The T-CY welcomed Ms Brigitte MABANDLA, Minister of Justice and Constitutional Development of the Republic of South Africa, who informed the T-CY about the current state of legislation in South Africa concerning cybercrime.

II. EXCHANGE OF VIEWS ON THE PRESENT SITUATION CONCERNING THE CONVENTION ON CYBERCRIME [ETS NO 185] AND ITS ADDITIONAL PROTOCOL [ETS NO. 189]

a. State of signatures, ratification and accession

i. General matters

7. The T-CY took note of the current state of signatures and ratifications of the Convention on cybercrime **(see Appendix III)**. It underlined the fact that very many non-European States have also shown considerable interest in the provisions of the Convention and that, at a world level, virtually all new legislation and draft legislation follow closely the provisions of the Convention.

8. The T-CY in particular:

- welcomed the growing and widespread international support for the Convention;

- noted that those States, which were not already Parties to the Convention were closely examining the provisions of the Convention and most of these States intended to become Parties as soon as possible in particular in order to be able to make full use of the procedural provisions concerning international co-operation. Austria, Germany, Ireland, Italy, Spain and the United Kingdom were likely to become Parties in 2008;

- noted that since its last meeting Slovakia had become a Party to the Convention, Georgia had signed the Convention on 1 April and Azerbaijan intended to sign the Convention in the first half of 2008;

- took note of the legislative and other steps being taken by States in order to become Parties to the Convention, recognised that the delay in ratification was usually due to the sometimes

lengthy legislative processes and encouraged these States to speed up the ratification process;

- noted that Costa Rica and Mexico had been invited to accede to the Convention, the Philippines would be invited to accede and the Dominican Republic had made a request to be invited to accede;

9. The T-CY took note of the current state of signatures and ratifications of the Additional Protocol to the Convention on cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems [ETS n° 189] (hereinafter the "Protocol") (**see Appendix IV**) and welcomed the signature of this Protocol by the Minister of Justice and Constitutional Development of South Africa.

10. The T-CY welcomed the information relating to cybercrime contacts and co-operation with the following non-European countries: Argentina, Australia, Bahrain, Botswana, Brazil, Colombia, Chile, China, Costa Rica, Dominican Republic, Egypt, India, Indonesia, Laos, Malaysia, Morocco, Nigeria, Peru, Philippines, Singapore, Sri Lanka, Trinidad and Tobago, Vietnam, and with regional organizations such as the Organisation of American States (OAS).

11. The T-CY encouraged States and international organizations or other bodies to promote the Convention in particular in those States with which they have historical links or special relationships or with States in the same region.

ii. Contact points

12. The T-CY reminded States to provide, before or when becoming Parties to the Convention, all relevant information required under the provisions of the Convention and, in particular, concerning the point of contact for the 24/7 network under Article 35.

13. The T-CY called on Armenia, Bosnia and Herzegovina and Ukraine, which are Parties to the Convention, to establish such contact points as a matter of urgency. The T-CY invited States to inform the Council of Europe of any changes concerning contact points.

14. The T-CY agreed to merge the Directory of Contact Points of the G8 Lyon-Roma High-tech Crime Subgroup and the list of contact points established under the Convention.

15. Furthermore the T-CY underlined the need to strengthen the effective operation of contact points and to consider the need for specialized judicial authorities and prosecutors. The T-CY requested the Consultative Council of European Prosecutors (CCPE) and EUROJUST to consider this matter further.

16. The T-CY requested the Project on cybercrime to prepare, in co-operation with the Committee of experts on the operation of European Conventions on co-operation in criminal matters (PC-OC) and the G8 Network:

- a report dealing in particular with the nature, role, powers, legal basis and institutional e-mail addresses of contact points and to submit it to the next meeting of the T-CY.

iii. Translations of the Convention

17. In addition to the original languages (English and French) the cybercrime website currently contains translations in the following 12 languages (Arabic, Dutch, German, Hungarian, Italian, Indonesian, Portuguese, Romanian, Russian, Slovak, Spanish and Turkish – see the website).

18. The T-CY invited participants to send the Secretariat translations of the Convention into other languages so that these translations could be included on the website and provide assistance to persons and States requiring such translations.

b. Implementation of the Convention in national legislation – Consideration of the implementation of Article 1.d concerning the definition of traffic data and of Article 2 concerning illegal access to computer systems

i. Traffic data

19. The T-CY agreed that it was necessary to make a clear distinction between traffic data as defined in Article 1.d of the Convention and content data.

ii. Illegal access

20. The representative of the European Commission informed the T-CY that the European Commission would publish a detailed report in May or June this year on the implementation of the Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems. This will include information on how EU member States implemented provisions on illegal access.

c. Consideration of the replies of the Parties to the questionnaire on the practical implementation of the Convention

21. The T-CY took note of the replies to the above questionnaire sent by the following: Bulgaria, Germany, Hungary, Romania, Russia, Slovakia, United States. The Committee requested those Parties which had not done so or those Parties wishing to update their replies to send their replies as soon as possible to the Secretariat.

22. The T-CY decided to consider these replies at its next meeting.

d. Consideration of specific difficulties arising out of international co-operation between the Parties / between Parties and other States

23. One particular difficulty pointed out by the T-CY was the question of the effective follow up to requests for expedited preservation and other preliminary measures through formal requests for mutual legal assistance. It was proposed, among other things, that 24/7 contact points and competent authorities for mutual legal assistance should strengthen their cooperation with each other.

e. Mutual legal assistance in computer related cases

24. The T-CY thanked the PC-OC for providing information concerning mutual legal assistance in computer-related cases from the following States: Armenia, Bosnia and Herzegovina, Bulgaria, Canada, Greece, Hungary, Latvia, Luxembourg, Malta, Poland, Portugal, Romania, Slovakia, Slovenia, Switzerland and Sweden. The T-CY was informed that the PC-OC would obtain additional replies and the T-CY agreed to examine these replies at its next meeting.

25. The T-CY noted that the 2nd Additional Protocol to the Convention on mutual assistance in criminal matters [ETS No 182] is very useful for co-operation in the field of cybercrime as it enables direct contacts between the authorities of the Parties to take place.

26. In addition the T-CY recognized that useful mutual assistance could also be provided by the PC-OC contact points, EUROJUST and the European Judicial Network.

27. The T-CY took note of a proposal by Romania concerning the preparation by the T-CY of a checklist for use between the 24/7 contact points for requests for expedited preservation of computer data and requested the Project on cybercrime to present a draft for consideration by the T-CY at its next meeting.

f. Difficulties to ascertain the location of servers and owners

28. The T-CY noted that sometimes it could be very difficult to locate servers and identify the owners of the servers and delay in locating servers could prevent law enforcement from taking action in sufficient time and Mr Gareth Sansom (Canada) made a PowerPoint presentation on the problem of location: cyberspace versus geographic space which provided much useful information on this matter.

29. The T-CY recognized that many jurisdictional difficulties arose owing to the ease by which servers could be changed rapidly from country to country or make use of Bots. The T-CY agreed that further consideration should be given to questions of jurisdiction in the light of technological developments and invited the Project on cybercrime to submit a report on this matter to the next meeting of the T-CY.

g. Consideration of establishing common rules for ISPs and their relations with law enforcement

30. See IIIb. below

h. Available training (by international bodies or by States)

31. The T-CY recognized that, although the Convention provides a comprehensive legal solution for all States, serious technical problems also have to be considered and training (police, prosecutors, judges and lawmakers) is particularly important to fight cybercrime.

32. The T-CY regretted that there was no overall data base indicating the training available at an international level but noted that the European Police Office (EUROPOL) and the European Police College (CEPOL) were working closely together to provide training for European Union States.

33. The T-CY underlined the need to provide appropriate forensic training in cybercrime not only for police officers but also to judges and prosecutors. The T-CY therefore invited the Consultative Council for European Prosecutors (CCPE) and the Consultative Council for European Judges (CCJE) to consider this matter.

i. Examples of public and private partnerships for the purpose of blocking of websites in the light of the recent relevant work carried out by the Council of Europe (Recommendation CM/Rec(2007)16 and Recommendation CM/Rec(2008)6)

34. The T-CY took note of Recommendation CM/Rec(2007)16 of the Committee of Ministers on measures to promote the public service value of the Internet (see in particular part V on security to the Appendix to the Recommendation which provides that “Member States should engage in international legal co-operation as a means of developing and strengthening security on the Internet and observance of international law in particular by: …..-promoting the safer use of the Internet and of ICTs, particularly for children, fighting against illegal content and tackling harmful and, where necessary, unwanted conduct through regulation, the encouragement of self-regulation, including the elaboration of codes of conduct, and the development of adequate technical standards and systems.”

35. The T-CY also took note of Recommendation CM/Rec(2008)6 of the Committee of Ministers on measures to promote the respect for freedom of expression and information with regard to Internet filters. It noted in particular the Appendix to the Recommendation which contains the following Guidelines:

    - using and controlling Internet filters in order to fully exercise and enjoy the right to freedom of expression and information;

    - appropriate filtering for children and young people;
    - use and application of Internet filters by the public and private sector.

j. Statistics concerning the extent of cybercrime and reports from international bodies or States

36. The T-CY recognized the importance of ascertaining the extent of cybercrime and the likely areas of growth in the future. Such information enabled States to plan for the future in particular concerning the necessary human and financial resources. This information was essential in order to take sufficient steps to deal with serious crime on the Internet.

37. The T-CY was informed that a proposal had been made by France to the European Union to collect statistics on different types of crime.

III INFORMATION CONCERNING THE PROJECT ON CYBERCRIME

a. Activities to date and work plan

38. The T-CY noted the progress made under the Project on cybercrime which was launched in September 2006 and has since helped to establish the Convention as a global guideline for the development of cybercrime legislation and a framework for international co-operation. In addition to European countries, it has so far supported legislative work in a wide range of countries and detailed analyses for Argentina, Brazil, Colombia, Egypt, India, Indonesia, Nigeria and Philippines.

39. The project is currently funded from the budget of the Council of Europe and voluntary contributions from Estonia and Microsoft. The T-CY called on other States and bodies to make additional contributions available so that the Project can be fully implemented.

b. Octopus Interface Conference "Co-operation against cybercrime" (1 and 2 April 2008) and its guidelines for co-operation between law enforcement and Internet service providers in the investigation of cybercrime

40. Many T-CY participants had attended the above Conference which took place in Strasbourg on 1 and 2 April 2008 as part of the Project on cybercrime. For the Conference conclusions (**See Appendix VI**).

41. The T-CY welcomed the results of this global Conference and took note of the several reports prepared under the Project. It welcomed the organization of the Project's global conference immediately prior to the T-CY and recommended that this practice be continued in the future if possible.

42. The T-CY took note of the adoption by the Conference of the non-binding Guidelines for co-operation between law enforcement and internet service providers in the investigation of cybercrime (**see Appendix V to this report**). The T-CY recognized that they could be useful to promote co-operation in this field.

c. Country profiles

43. The T-CY welcomed the following 27 country profiles on cybercrime legislation which have been included on the website: Albania, Argentina, Armenia, Austria, Brazil, Bulgaria, Italy, China, Croatia, Cyprus, Czech Republic, Dominican Republic, France, Germany, Hungary, Lithuania, Morocco, Mexico, Moldova, Portugal, Romania, Slovak Republic, "the former Yugoslav Republic of Macedonia", The Philippines, Turkey, Ukraine, The United States of America.

44. The T-CY underlined the usefulness of the country profiles as a tool for analyzing the implementation of the Convention in national law as well as for the exchanges of good practices and experience.

45. The T-CY encouraged participants to contribute to the preparation and, where necessary, to the updating of the profiles concerning their States.

IV. EXCHANGE OF VIEWS ON CO-OPERATION BETWEEN STATES, INTERNATIONAL ORGANISATIONS, ACADEMIA AND THE PRIVATE SECTOR

46. The T-CY underlined the need to promote public and private partnerships in order to fight cybercrime and noted that such partnerships could play an important role in preventing the criminal use of the Internet.

47. The desirability of close co-operation between the T-CY and the G8 Lyon-Roma High-Tech Crime Subgroup was stressed in particular to ensure proper co-ordination between the contact points for the 24/7 network.

V. OTHER WORK CARRIED OUT BY THE COUNCIL OF EUROPE CONCERNING SPECIFIC MATTERS RELATING TO CYBERCRIME

a. Second Meeting of the Internet Governance Forum (IGF) (Rio de Janeiro, 12 - 15 November 2007) and preparations for the third IGF meeting (Hyderabad, India, 3 – 6 December 2008)

48. The Secretariat provided information about the 2007 IGF meeting and that the Council of Europe was the most active and visible intergovernmental organization present and provided the leading voice in much of the discussion concerning cybercrime, protecting children, the right to privacy and democratic participation on the Internet.

49. The Council of Europe had organized 15 events on the openness, security, access, diversity and critical Internet resources of the Internet, including two events specifically related to the Convention on cybercrime which, as a result, gained much publicity. A number of countries from South America showed a strong interest in acceding to the Convention and countries from other regions showed a serious interest in the Convention and for a direct bilateral follow-up with the Council of Europe..

50. The T-CY was informed that the Council of Europe is now preparing its participation at the next IGF meeting which will take place in Hyderabad (India), from 3 to 6 December 2008. India and a number of other countries could accede to the Convention on cybercrime during this meeting.

51. The Secretariat invited:

- participants in the T-CY to send it any suggestions for matters to be considered at the next IGF;

- those persons who would attend the IGF on behalf of their States or organizations to contact it in order to ensure maximum co-ordination and efficiency in the field of cybercrime.

b. Opening for signature of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.: 201)

52. The T-CY was informed about the above recent Convention which had been signed by 27 States.

53. The briefing to the T-CY noted in particular the following articles of the above Convention:

- Article 6, which deals with education for children, requires Parties to provide children with information on the situations of risk of sexual exploitation and sexual abuse especially those involving the use of new information and communication and communication technologies;
- Article 20, which deals with offences concerning child pornography, is very similar to Article 9 of the Convention on cybercrime but, unlike Article 9, it is not restricted to offences committed through a computer system. In addition Article 20 requires Parties, unless they have made a reservation, to criminalise "knowingly obtaining access, through information and communication technologies, to child pornography";
- Article 30, which contains principles concerning investigation, prosecution and procedural law, requires Parties to take measures to identify victims "in particular by analyzing child pornography material, such as photographs and audiovisual recordings transmitted or made available through the use of information and communication technologies.

c. Information concerning the work of the Group of Specialists on Counterfeit Pharmaceutical Products (PC-S-CP)

54. The T-CY was informed that, owing to the widespread circulation of counterfeit medicines and the absence in many countries of effective criminal sanctions, the PC-S-CP was preparing texts to ensure, *inter alia*, that such acts are properly criminalized. These texts would, subject to further approval by the relevant bodies within the Council of Europe, be included in a convention. Full account would be taken of the Convention on Cybercrime.

55. Any future Convention in this field should be open to all States and participation by non-European countries encouraged.

d. Opinion of CODEXTER on cyberterrorism and the use of the Internet for terrorist purposes

56. The T-CY took note of the above opinion of CODEXTER which was transmitted to the T-CY by the Committee of Ministers.

57. The opinion of CODEXTER in particular encouraged States to become Parties to the Convention on Cybercrime and indicated: "The effective implementation of the Cybercrime Convention would ensure that national legislation provides appropriate sanctions for cases involving serious attacks, including terrorist ones, on IT-based or IT-general infrastructures."

58. The T-CY noted the different views on the need for a specific instrument in this field.

VII ANY OTHER BUSINESS

59. The T-CY took note of the decisions adopted by the European Committee on crime problems (CDPC) at its 56th meeting concerning matters relating to cybercrime.

VIII. NEXT MEETING OF THE CYBERCRIME CONVENTION COMMITTEE (T-CY)

60. The T-CY agreed to hold its next meeting in March 2009, if possible immediately following an Octopus Conference on cybercrime.

61. The T-CY agreed to include the following items on its agenda:

    a. state of signatures, ratifications and accession to the Convention and its Protocol (including progress made and likely timetable)
    b. report concerning contact points (to be prepared by the Project on cybercrime)
    c. replies from Parties concerning the practical implementation of the Convention
    d. legal assistance in computer related cases
    e. check list for use between the 24/7 contact points for requests for expedited preservation of computer data (to be prepared by the Project on cybercrime)
    f. report on questions of jurisdiction in the light of technical developments which enable servers to be changed rapidly from country to country (to be prepared by the Project on cybercrime)

62. The T-CY agreed to invite to its next meeting all the categories of participants invited to its present meeting. In addition the committee considered that it would be useful to consider inviting States interested in acceding to the Convention and other international intergovernmental organizations.

63. The T-CY therefore invited all participants in the present meeting to send the Secretariat proposals concerning possible additional categories of participants at its next meeting. Participants are invited to send their proposals to the Secretariat (DG1.cybercrime@coe.int) not later than 1 September 2008.

APPENDIX I

LIST OF PARTICIPANTS / LISTE DE PARTICIPANTS

PARTICIPATING PARTIES TO THE CONVENTION ON CYBERCRIME
PARTIES PARTICIPANT A LA CONVENTION SUR LA CYBERCRIMINALITE

BULGARIA / BULGARIE

M. Krassimir BOJANOV, Adjoint au Représentant permanent de la Bulgarie auprès du Conseil de l'Europe, STRASBOURG, France

CROATIA / CROATIE

Mr Ivan MIJATOVIC, Chief inspector, Ministry of the Interior, ZAGREB, Croatia

ESTONIA / ESTONIE

Mr Markko KÜNNAPU, Adviser, Criminal Police Department, Ministry of Justice, TALLINN, Estonia

FINLAND / FINLANDE

Mr Antti PIHLAJAMÄKI, Chief District Prosecutor, Prosecutor's Office of South-West Finland, TURKU, Finland

FRANCE

M. Fabien LANG, Commissaire de Police, Adjoint au Chef de l'OCLCTIC, Direction centrale de la Police Judiciaire, NANTERRE, France

Mme Setareh Marie AGHA BABAEI, Stagiaire, Direction Centrale de la police judiciaire (OCLCTIC), NANTERRE, France

HUNGARY / HONGRIE

Mr Zsolt SZABOLCSI, Senior detective, National Bureau of Investigation, High-tech Crime Department, BUDAPEST, Hungary

Ms Eszter VICZKO, Legal Adviser, Ministry of Justice, BUDAPEST, Hungary

ICELAND / ISLANDE

Ms Ragna ÁRNADÓTTIR, Director of Legal Affairs, Ministry of Justice and Ecclesiastical Affairs, REYKJAVÍK, Iceland; *Apologised / Excusé*

Mr Gunnar Narfi GUNNARSSON, Legal Expert, Directorate of Legal Affairs, Ministry of Justice and Ecclesiastical Affairs, REYKJAVÍK, Iceland; *Apologised / Excusé*

NETHERLANDS / PAYS-BAS

Mr Henrik W. K. KASPERSEN, Director Computer/Law Institute, Vrije Universiteit, De Boelelaan AMSTERDAM, The Netherlands

NORWAY / NORVEGE

Mr Erik MOESTUE, Police Prosecutor, National Criminal Investigation Service (NCIS), OSLO, Norway

ROMANIA / ROUMANIE

Ms Cristina SCHULMAN, Vice Chair of the Committee, Legal adviser – Department for International Law and Treaties Ministry of Justice, BUCHAREST, Romania

Ms Ioana Bogdana ALBANI, Chief Prosecutor, Head of the Cybercrime Unit, Prosecutor's Office attached to the High Court of Cassation and Justice, Directorate for the Investigation of Organised Crime and Terrorism, BUCHAREST, Romania

SLOVAKIA / SLOVAQUIE

Mr Miroslav TIZA, Prosecutor, The General's Prosecutors Office of the Slovak Republic, International Department, BRATISLAVA, Slovak Republic

UKRAINE

Mr Andrii FIALKOVSKYI, Advisor, National Security Council, KIEV, Ukraine

UNITED STATES OF AMERICA / ETATS-UNIS D'AMÉRIQUE

Ms Betty SHAVE, Chair of the Committee, Assistant Deputy Chief for International Computer Crime, Computer Crime and Intellectual property Section, US Department of Justice, WASHINGTON, DC

Mr Thomas DUKES, Trial Attorney, US Department of Justice, Computer Crime and Intellectual Property Section, WASHINGTON DC

OTHER PARTICIPANTS / AUTRES PARTICIPANTS

AZERBAÏJAN / AZERBAIDJAN

Mr Bakhtiyar N. MAMMADOV, Head of Legal and Human Resources Department, Ministry of Communications and Information Technologies, BAKU, Republic of Azerbaijan

CANADA

Mr Gareth SANSOM, Director, Technology & Analysis, Ministry of Justice, OTTAWA, Canada

CZECH REPUBLIC / REPUBLIQUE TCHEQUE

Mr Tomáš HUDEČEK, Ministry of Justice, International Section, PRAGUE 2, Czech Republic

GEORGIA / GEORGIE

Mr Levan JANIKASHVILI, Deputy Head of Operative, Technical Department, Ministry of Internal Affairs of Georgia, TBILISI, Georgia

Ms Natia GVAZAVA, Head of International Cooperation Unit, Ministry of Internal Affairs of Georgia, TBILISI, Georgia

GERMANY / ALLEMAGNE

Mr Alexander DÖRRBECKER, Deputy Head of Division, Federal Ministry of Justice, BERLIN, Germany

Ms Ivonne SCHWINDT, Assistant, Federal Ministry of Justice, BERLIN, Germany

GREECE / GRECE

Mr Theodoros MITRAKOS, Solicitor, Ministry of Justice, ATHEN, Greece; Apologised / Excusé

HOLY SEE / SAINT SIEGE

Apologised / Excusé

JAPAN / JAPON

Mr Shoichi ITO, Senior Superintendent, Cybercrime Division, Community Safety Bureau, National Police Agency, 2TOKYO, Japan

Mr Hiroyuki OSHIMA, Official, International Organized Crime Division, Foreign Policy Bureau, Ministry of Foreign Affairs, TOKYO, Japan

Mr Akira TAKANO, Consul (Attorney), Consulate General of Japan, STRASBOURG, France

MEXICO / MEXIQUE

Mr Rodrigo LABARDINI FLORES, Deputy Legal Adviser “B”, Ministry of Foreign Affairs, MEXICO CITY, Mexico

Mr Guillermo VALLS ESPONDA, Agregado Legal para la Unión Europea y Suiza, Procuraduría General de la República / Embajada de México en España, MADRID, Spain

Mr J. Iván FLORES CONTRERAS, Liaison Office for EU of Ministry of Public Safety of Mexico, Mexico Embassy in Spain, ,MADRID, Spain

MOLDOVA

Mr Valentin COLIBAN, Deputy Chief of Informatization Directorate, Ministry of Informational Development, Chisinau, Republic of Moldova

PORTUGAL

Mr Pedro VERDELHO, Docente, Centre for Judiciary Studies, LISBOA, Portugal

RUSSIAN FEDERATION / FEDERATION DE RUSSIE

Mr Boris MIROSHNIKOV, Head of Department “K”, Ministry of Interior, MOSCOW, Russian Federation

Mr Mikhail SHURGALIN, Head of Section, Department of New Challenges and Threats, Ministry of Foreign Affairs, MOSCOW, Russian Federation

SPAIN / ESPAGNE

Mr Antonio ROMA VALDES, Public Prosecutor, Fiscalia SCI, Fiscalia de Santiago, SANTIAGO, Spain

Mr Luis Maria URIARTE VALIENTE, Prosecutor, Fiscalia General Del Estado, Fiscalia Provincial de Pontevedra, PONTEVEDRA, Spain

SWITZERLAND / SUISSE

Mme Christine MAGNIN, Unité Droit pénal international, Office fédéral de la Justice, BERNE, Switzerland

M. Nicolas BOTTINELLI, Unité entraide judiciaire, Office fédéral de la Justice, BERNE, Suisse

M. Mauro VIGNATI, Analyste Cybercrime, Federal Office of Police, BERN, Switzerland

Mr Adrian KOSTER, Juriste, Federal Office of Police, BERN, Switzerland;

TURKEY / TURQUIE

Mr Osman NIHAT SEN, Head of the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Mr Erol AKTAY, Communications Expert at the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Mr Dogan KILINC, Communications Expert at the Internet Department of the Telecommunications Authority, ANKARA, Turkey

Ms Özlem ALLIOĞLU, Lawyer, Radio and Television Supreme Council, ANKARA, Turkey

Mr Soner BASLI, System Analyst, Radio and Television Supreme Council, ANKARA, Turkey

Mr Nihat ÇAYLAK, Expert, Radio and Television Supreme Council, ANKARA, Turkey

UNITED KINGDOM / ROYAUME-UNI

Apologised / Excusé

EUROPEAN COMMITTEE ON CRIME PROBLEMS / COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS (CDPC)

Mr Branislav BOHÁČIK, Head of Division for Judicial Co-operation in Criminal Matters, Ministry of Justice, BRATISLAVA, Slovak Republic

STEERING COMMITTEE ON THE MEDIA AND NEW COMMUNICATION SERVICES / COMITE DIRECTEUR SUR LES MEDIAS ET LES NOUVEAUX SERVICES DE COMMUNICATION (CDMC)

M. Thomas SCHNEIDER, Service des Affaires internationales, Office fédéral de la communication, BIENNE, Suisse

INTERNATIONAL TELECOMMUNICATION UNION (ITU) / UNION INTERNATIONALE DES TELECOMMUNICATIONS (UTI)

Mr Alexander NTOKO, Head, Corporate Strategy Division, International Telecommunication Union GENEVA, Switzerland

ORGANISATION FOR SECURITY AND CO-OPERATION IN EUROPE (OSCE) ACTION AGAINST TERRORISM UNIT (ATU) / ORGANISATION POUR LA SECURITE ET LA COOPERATION EN EUROPE (OSCE) UNITE D'ACTION CONTRE LE TERRORISME (UAT)

Mr Nemanja MALISEVIC, CTN Co-ordinator, Assistant Programme Officer, Organization for Security and Co-operation in Europe, VIENNA, Austria

Mr Joseph MANGAN, Information Management Officer, Strategic Police Matters Unit, Organization for Security and Co-operation in Europe, OSCE VIENNA, Austria

UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC) / OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC)

Mr Gillian MURRAY, Focal Point for Cybercrime, Division for Treaty Affairs, United Nations Office on Drugs and Crime, VIENNA, Austria

Mr Chang SOO LEE, Division for Treaty Affairs(DTA), Treaty and Legal Assistance Branch(TLAB/OCS), United Nations Office on Drugs and Crime, VIENNA, Austria

EUROPEAN COMMISSION / COMMISSION EUROPEENNE

Mr Michael CARLIN, European Commission, Head of Sector, BRUSSELS, Belgium

EUROPOL

Mr Nicola DILEONE, First Officer, Europol, OC Groups Unit/ High Tech Crime Centre, THE HAGUE, The Netherlands

SECRETARIAT OF THE COUNCIL OF EUROPE
SECRETARIAT DU CONSEIL DE L'EUROPE

Council of Europe - Directorate General of Human Rights and Legal affairs
DG-HL
Conseil de l'Europe - Direction des droits de l'Homme et des affaires juridiques

T-CY – Contacts
Website: www.coe.int/cybercrime
Telephone of the Secretariat: +33 3 90 21 50 35

Ms Margaret KILLERBY, Secretary a.i. to the T-CY, Head of Law Reform Department a.i., Director of Co-operation

Mr Alexander SEGER, Head of Economic Crime Division, Technical Co-operation Department, Directorate of Co-operation

Mr Carlo CHIAROMONTE, Head of Criminal Law Division, Law Reform Department

Mr Lee HIBBARD, Coordinator of International Information Society, Media and Information Society Division

Mr David DOLIDZE, Administrator, Gender Equality and Anti-Trafficking Division

Ms Dominique WULFRAN, Assistant, Law Reform Department

INTERPRETERS / INTERPRETES

Mme Isabelle MARCHINI
Mme Pascale MICHLIN

APPENDIX II

AGENDA / *ORDRE DU JOUR*

1. **Opening of the meeting / *Ouverture de la réunion***

   Working documents / *Documents de travail*:

   - Information document concerning the T-CY / *Document d'information concernant le T-CY* T-CY(2008) INF 01
   - Report of the second meeting of the Cybercrime Convention Committee / *Rapport de la deuxième réunion sur le Comité de la Convention Cybercriminalité* T-CY(2007)03

2. **Election of the Chair and Vice-Chair by representatives of States Party to the Convention / Election du Président et du Vice-Président par les représentants des Etats Parties à la Convention**

3. **Adoption of the agenda / Adoption de l'ordre du jour**

4. **Exchange of views on the present situation concerning the Convention on Cybercrime (CETS No.:185) and its Additional Protocol (CETS No.:189) / *Echange de vues sur la situation actuelle concernant le Convention sur la cybercriminalité (STCE no. :185) et son Protocole additionel (STCE no. :189)***

   a. State of signatures, ratifications and accession to the Convention and its additional Protocol (including progress made and likely future timetable) / *Etat des signatures, ratifications, adhésions à la Convention et à son protocole additionnel (y compris l'état d'avancement et le calendrier prévisionnel);*

   b. Implementation of the Convention in national legislation – Consideration of the implementation of Article 1.d concerning the definition of traffic data and of Article 2 concerning illegal access to computer systems / *Mise en œuvre de la Convention dans la législation nationale – examen de l'article 1.d concernant la définition des données relatives au trafic et de l'article 2 concernant a l'accès illégal aux systèmes informatiques ;*

   c. Consideration of the replies of the Parties to questions on the practical implementation of the Convention / *Considération des réponses des Parties aux questions concernant la mise en œuvre pratique de la Convention*;

   d. Consideration of specific difficulties arising out of international co-operation / *Examen de problèmes spécifiques découlant de la coopération internationale:*

      - between the Parties / *entre les Parties*
      - between Parties and other States / *entre les Parties et d'autres Etats*;

   e. Mutual legal assistance in computer related cases in particular in urgent cases in the light of information provided by the CDPC and the PC-OC, and consideration of the implementation of Articles 16 and 17 on expedited preservation of the Convention on Cybercrime (see paragraphs 21 – 25 of T-CY (2007)03) / *Entraide judiciaire dans les affaires informatiques, notamment en cas d'urgence, à la lumière des informations fournies par le CDPC et le PC-OC, et examen de la mise en œuvre des Articles 16 et 17*

sur la conservation rapide de la Convention sur la cybercriminalité (voir paragraphes 21 - 25 de T-CY (2007)03);

f. Difficulties to ascertain the location of servers and owners (see paragraph 34 of T-CY (2007)03) / *Difficultés à déterminer la localisation des serveurs et des propriétaires (voir paragraphe 34 de T-CY (2007)03)*;

g. Consideration of establishing common rules for ISPs and their relations with law enforcement, in the light of the Study prepared under the Project on Cybercrime (see also paragraph 16 of T-CY (2007)03) / *Examen d'établissement des règles communes pour les FAI et leurs relations avec les services de répression à la lumière d une étude préparée sous l'autorité du Projet sur la Cybercriminalité (voir aussi paragraphe 16 de T-CY (2007)03)*;

h. Available training (by international bodies or by States) (see paragraph 14 of T-CY (2007)03) / *Formations proposées (par les instances internationales ou les Etats) (voir paragraphe 14 de T-CY (2007)03)*;

i. Examples of public and private partnerships for the purpose of blocking of websites in the light of the recent relevant work carried out by the Council of Europe (Recommendation CM/Rec(2007)16 and Recommendation CM/Rec(2008)6) (see paragraph 29 of T-CY (2007)03) / *Exemples de partenariats publics et privés pour le blocage des sites Web, à la lumière des travaux récents menés au Conseil de l'Europe (Recommandation CM/Rec(2007)16 et Recommandation CM/Rec(2008)6) (voir paragraphe 29 de T-CY (2007)03)* ;

j. Statistics concerning the extent of cybercrime and reports from international bodies or States (see paragraphs 40 and 41 of T-CY (2007)03) / *Statistiques concernant l'étendue de la cybercriminalité et rapports des instances internationales ou des Etats (voir paragraphes 40 et 41 de T-CY (2007)03)*.

Working documents / *Documents de travail*:

- Information document concerning the T-CY /
  Document d'information concernant le T-CY (item/*point* 4.a) T-CY(2008) INF 01

- Report of the second meeting of the Cybercrime Convention Committee
  / *Rapport de la deuxième réunion sur le Comité*
  de la Convention Cybercriminalité (items/*points* 4. b, c, d, e, f, g, h, I, j, k)
  T-CY(2007)03

- The Convention on Cybercrime (CETS No.:185) and its explanatory report
  La Convention sur la Cybercriminalité (STCE no. :185) et son rapport explicatif
  (items/*points* 4.a, b, c, d, e, f, g)*;*

- The Protocol to the Convention (CETS No.:189) and its explanatory report
  Le Protocole à la Convention (STCE no. :189) et son rapport explicatif
  (items/*points* 4.a, b, c, d, e, f, g) *;*

- Replies of the Parties to questionnaire concerning
  the practical implementation of the Convention /
  Réponses des états Parties au questionnaire
  sur la mise en oeuvre de la Convention (item/*point* 4.c) T-CY (2008)01

- Replies to the questionnaire of the PC-OC concerning mutual legal assistance
  in computer related cases /

Réponses au questionnaire du PC-OC sur l'entraide judiciaire dans les affaires liées à l'informatique (item/*point* 4.e) PC-OC (2007) 15 PROV

- Recommendation CM/Rec(2007)16 of the Committee of Ministers to member states on measures to promote the public service value of the Internet / *Recommandation CM/Rec(2007)16 du Comité des Ministres aux Etats membres sur des mesures visant à promouvoir la valeur de service public de l'Internet* (item/*point* 4.i)

- Recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to Internet filters / *Recommandation CM/Rec(2008)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet* (item/*point* 4.i)

- "National legislation implementing the Convention on Cybercrime - Comparative analysis and good practices", prepared by Prof. Dr. Lorenzo Picotti, Law University of Verona (Italy) – English only (item 4.b)

- "The effectiveness of international co-operation against cybercrime: examples of good practice", prepared by Pedro Verdelho (Portugal)– English only (item 4.e)

- "Guidelines for the cooperation between law enforcement and internet service providers against cybercrime", prepared by Cormac Callanan (Ireland) Marco Gercke (Germany) – English only (item 4.g)

5. Information concerning the Project on Cybercrime / *Informations concernant le Projet sur Cybercriminalité*

a. Activities to date and workplan 2008 / *Les activités à ce jour et le programme des travaux 2008*

Working documents / *Documents de travail*:

- Progress Report of the Project on Cybercrime / *Rapport de Progrès de Projet sur la Cybercriminalité*
- Report of the second meeting of the Cybercrime Convention Committee / *Rapport de la deuxième réunion du Comité de la Convention Cybercriminalité* , T-CY(2007)3
- *Studies prepared under the Project on Cybercrime / Les études préparées sous le Projet sur la Cybercriminalité*

b. Octopus Interface Conference « Co-operation Against Cybercrime », 1-2 April 2008 / *la Conférence Octopus Interface « Coopération contre le Cybercriminalité », 1-2 avril 2008 ;*

c. Country Profiles / Les profiles des états

6. Exchange of views on co-operation between States, international organisations, academia and the private sector / *Echange de vues sur la coopération entre les Etats, les organisations internationales, le milieu de la recherche et le secteur privé*

Working documents / *Documents de travail*:

- Report of the second meeting of the Cybercrime Convention Committee / *Rapport de la deuxième réunion du Comité de la Convention* Cybercriminalité T-CY(2007)3

- Cybercrime and the European Union / *La Cybercriminalité et* l'Union *Européenne*
  T-CY(2007)02

7. Other work carried out in the Council of Europe concerning specific matters relating to cybercrime / *Autres travaux menés par le Conseil de l'Europe sur des sujets spécifiques relatifs à la cybercriminalité*

a. Information concerning the Second Meeting of the Internet Governance Forum (IGF), Rio de Janeiro, 12 - 15 November 2007 and preparations for the Third IGF meeting in New Delhi, December 2008 / Les informations sur "Internet Governance Forum", Rio de Janeiro, 12-15 novembre 2007 et les préparations pour la troisième réunion a New Delhi, décembre 2008

Working documents / *Documents de travail:*

- Summary of the Chairman of the Second Meeting of the IGF / Sommaire du Président de la Deuxième Réunion du IGF

b. Opening for signature of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS No.: 201) / *Ouverture à la signature de la Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels (STCE no. : 201)*

Working documents / *Documents de travail:*

- Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and its Explanatory Report / Convention du Conseil de l'Europe pour la protection des enfants contre l'exploitation et les abus sexuels et son Rapport Explicatif ;

c. Information concerning the work of the Group of Specialists on Counterfeit Pharmaceutical Products (PC-S-CP) / *Information concernant les travaux du Groupe de Spécialistes sur les Produits Pharmaceutiques Contrefaits (PC-S-CP)*

Working documents / *Documents de travail:*

- Final Report of the PC-S-CP / Rapport Final du PC-S-CP

d. Opinion of CODEXTER on cyberterrorism and use of the Internet for terrorist purposes / *Avis du CODEXTER sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes*

Working documents / *Documents de travail:*

- Information Document concerning the Opinion
  of CODEXTER on cyberterrorism and use of Internet for terrorist purposes /
  Document d'information concernant l'avis du CODEXTER
  sur le cyberterrorisme et l'utilisation de l'Internet à des fins terroristes
  T-CY (2008) INF 02

8. Any other business / *Divers*

9. Next meeting of the Cybercrime Convention Committee (T-CY) / *Prochaine réunion du Comité de la Convention Cybercriminalité (T-CY)*

10. Adoption of the abridged meeting report / *Adoption du rapport abrégé de la réunion*

APPENDIX III

Convention on Cybercrime
CETS No.: 185

Treaty open for signature by the member States and the non-member States which have participated in its elaboration and for accession by other non-member States

Opening for signature

Place: Budapest
Date : 23/11/2001

Entry into force

Conditions: 5 Ratifications including at least 3 member States of the Council of Europe
Date : 1/7/2004

Status as of: 8/4/2008

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	23/11/2001	20/6/2002	1/7/2004				X			
Andorra										
Armenia	23/11/2001	12/10/2006	1/2/2007							
Austria	23/11/2001									
Azerbaijan										
Belgium	23/11/2001									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006				X			
Bulgaria	23/11/2001	7/4/2005	1/8/2005		X	X				
Croatia	23/11/2001	17/10/2002	1/7/2004							
Cyprus	23/11/2001	19/1/2005	1/5/2005							
Czech Republic	9/2/2005									
Denmark	22/4/2003	21/6/2005	1/10/2005		X		X	X		
Estonia	23/11/2001	12/5/2003	1/7/2004				X			
Finland	23/11/2001	24/5/2007	1/9/2007		X	X	X			
France	23/11/2001	10/1/2006	1/5/2006		X	X	X			
Georgia	1/4/2008									
Germany	23/11/2001									
Greece	23/11/2001									
Hungary	23/11/2001	4/12/2003	1/7/2004		X	X	X			
Iceland	30/11/2001	29/1/2007	1/5/2007		X		X			

Ireland	28/2/2002									
Italy	23/11/2001									
Latvia	5/5/2004	14/2/2007	1/6/2007		X		X			
Liechtenstein										
Lithuania	23/6/2003	18/3/2004	1/7/2004		X	X	X			
Luxembourg	28/1/2003									
Malta	17/1/2002									
Moldova	23/11/2001									
Monaco										
Montenegro	7/4/2005			55						
Netherlands	23/11/2001	16/11/2006	1/3/2007				X	X		
Norway	23/11/2001	30/6/2006	1/10/2006		X	X	X			
Poland	23/11/2001									
Portugal	23/11/2001									
Romania	23/11/2001	12/5/2004	1/9/2004				X			
Russia										
San Marino										
Serbia	7/4/2005			55						
Slovakia	4/2/2005	8/1/2008	1/5/2008		X	X	X			
Slovenia	24/7/2002	8/9/2004	1/1/2005				X			
Spain	23/11/2001 r									
Sweden	23/11/2001									
Switzerland	23/11/2001									
the former Yugoslav Republic of Macedonia	23/11/2001	15/9/2004	1/1/2005				X			
Turkey										
Ukraine	23/11/2001	10/3/2006	1/7/2006		X		X			
United Kingdom	23/11/2001									

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	23/11/2001									
Costa Rica										
Japan	23/11/2001									

Mexico										
South Africa	23/11/2001									
United States	23/11/2001	29/9/2006	1/1/2007		X	X	X			

Total number of signatures not followed by ratifications:	22
Total number of ratifications/accessions:	22

APPENDIX IV

Additional Protocol to the Convention on cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems
CETS No.: 189

Treaty open for signature by the States which have signed the Treaty ETS 185.

Opening for signature

Place: Strasbourg
Date : 28/1/2003

Entry into force

Conditions: 5 Ratifications.
Date : 1/3/2006

Status as of: 8/4/2008

Member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Albania	26/5/2003	26/11/2004	1/3/2006							
Andorra										
Armenia	28/1/2003	12/10/2006	1/2/2007							
Austria	30/1/2003									
Azerbaijan										
Belgium	28/1/2003									
Bosnia and Herzegovina	9/2/2005	19/5/2006	1/9/2006							
Bulgaria										
Croatia	26/3/2003									
Cyprus	19/1/2005	23/6/2005	1/3/2006							
Czech Republic										
Denmark	11/2/2004	21/6/2005	1/3/2006		X			X		
Estonia	28/1/2003									
Finland	28/1/2003									
France	28/1/2003	10/1/2006	1/5/2006			X				
Georgia										
Germany	28/1/2003									
Greece	28/1/2003									
Hungary										
Iceland	9/10/2003									
Ireland										
Italy										
Latvia	5/5/2004	14/2/2007	1/6/2007							
Liechtenstein										
Lithuania	7/4/2005	12/10/2006	1/2/2007			X				
Luxembourg	28/1/2003									

Malta	28/1/2003									
Moldova	25/4/2003									
Monaco										
Montenegro	7/4/2005			55						
Netherlands	28/1/2003									
Norway										
Poland	21/7/2003									
Portugal	17/3/2003									
Romania	9/10/2003									
Russia										
San Marino										
Serbia	7/4/2005			55						
Slovakia										
Slovenia	26/2/2004	8/9/2004	1/3/2006							
Spain										
Sweden	28/1/2003									
Switzerland	9/10/2003									
the former Yugoslav Republic of Macedonia	14/11/2005	14/11/2005	1/3/2006							
Turkey										
Ukraine	8/4/2005	21/12/2006	1/4/2007			X				
United Kingdom										

Non-member States of the Council of Europe

States	Signature	Ratification	Entry into force	Notes	R.	D.	A.	T.	C.	O.
Canada	8/7/2005									
Japan										
South Africa	4/4/2008									
United States										

Total number of signatures not followed by ratifications:	21
Total number of ratifications/accessions:	11

APPENDIX V

GUIDELINES

ADOPTED BY
THE CONFERENCE ON "CO-OPERATION AGAINST CYBERCRIME"
COUNCIL OF EUROPE, STRASBOURG, FRANCE 1 AND 2 APRIL 2008

FOR THE COOPERATION BETWEEN LAW ENFORCEMENT AND INTERNET SERVICE PROVIDERS AGAINST CYBERCRIME

These guidelines are the result of several rounds of discussions with representatives from industry and law enforcement who met between October 2007 and February 2008 under the auspices of the Council of Europe's Project on Cybercrime. They are complemented by a detailed background study.

The guidelines were further discussed and adopted by the global Conference "Cooperation against Cybercrime" (Council of Europe, Strasbourg, France) on 1-2 April 2008.

The guidelines are a non-binding tool that can now be disseminated and used to help law enforcement and service providers in any country around the world to organise their cooperation against cybercrime while respecting each others' roles and responsibilities as well as the rights of internet users.

Guidelines for the cooperation between law enforcement and internet service providers against cybercrime[2]

Introduction

1. Building an information society requires the strengthening of trust in information and communications technologies (ICT's), the protection of personal data and privacy, and the promotion of a global culture of cyber-security in a context where societies worldwide are increasingly dependent on ICT and thus vulnerable to cybercrime;

2. The First and Second World Summit on the Information Society (Geneva 2003, Tunis 2005) – among other things – committed to build an inclusive information society where everyone can create, access, utilize and share information and knowledge, achieve their potential and improve their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights, and which calls for new forms of partnerships and cooperation among governments, the private sector, civil society and international organisations;

[2] This document does not necessarily reflect official positions of the Council of Europe. For further information please contact Alexander.seger@coe.int

3. Internet service providers (ISP) and law enforcement authorities (LEA) play a crucial role in the realization of this vision;

4. National legislation in line with the Convention on Cybercrime of the Council of Europe (the "Budapest Convention") helps countries create a sound legal basis for public-private cooperation, investigative powers as well as international cooperation;

5. The guidelines are not intending to substitute existing legal instrument but assume adequate legal instruments exist that provide a well balanced system of investigation instruments as well as related safeguards and a protection of fundamental human rights such as freedom of expression, the respect for private life, home and correspondence and the right to data protection. It is therefore recommended that states adopt regulations in their national law in order to fully implement the procedural provisions of the Convention on Cybercrime, and to define investigative authorities and obligations of law enforcement while putting in place conditions and safeguards as foreseen in Article 15 of the Convention. This will

- ensure efficient work of law enforcement authorities
- protect the ability of Internet service providers to provide services
- ensure that national regulations are in line with global standards
- promote global standards instead of isolated national solutions
- help ensure due process and the rule of law, including principles of legality, proportionality and necessity;

6. For the purposes of these guidelines we use the definition of service provider included in the Convention on Cybercrime in Article 1 which defines "service provider" in a broad manner as meaning:

i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and

ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;

7. In order to enhance cybersecurity, minimise use of services for illegal purposes and build trust in ICT, it is essential that Internet service providers and law enforcement authorities cooperate with each other in an efficient manner with due consideration to their respective roles, the cost of such cooperation and the rights of citizens;

8. The purpose of the present guidelines is to help law enforcement authorities and Internet service providers structure their interactions in relation to cybercrime issues. They are based on existing good practices and should be applicable in any country around the world in accordance with national legislation and respect for the freedom of expression, privacy, the protection of personal data and other fundamental rights of citizens;

9. It is therefore recommended that States, law enforcement authorities and Internet service providers undertake the following measures at a national level:

Common guidelines

10. Law enforcement authorities and Internet service providers should be encouraged to engage in information exchange to strengthen their capacity to identify and combat emerging types

of cybercrime. Law enforcement authorities should be encouraged to inform service providers about cybercrime trends;

11. Law enforcement and Internet service providers should promote a culture of cooperation – rather than confrontation - including the sharing of good practices. Regular meetings in order to exchange experience and resolve problems are encouraged;

12. Law enforcement and service providers should be encouraged to develop written procedures for cooperation with each other. Where possible, both parties should be encouraged to provide structured feedback on the operation of these procedures to each other;

13. Formal partnerships between law enforcement and service providers should be considered in order to establish longer-term relationships with proper guarantees for both sides that the partnership will not infringe any legal rights on the side of the industry or interfere with any legal powers on the side of law enforcement;

14. Both law enforcement authorities and Internet service providers should protect the fundamental rights of citizens according to United Nations and other applicable European and international standards such as the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as well as domestic law. This places reasonable limits to the level of cooperation possible;

15. Law enforcement authorities and Internet service providers are encouraged to cooperate with each other in view of enforcing privacy and data protection standards at the domestic level but also with regard to cross-border data flows. The work of the Council of Europe and the OECD provides guidance in this respect;

16. Both sides should be mindful of the costs involved in creating and responding to requests. Procedures should be developed with consideration of the financial impact of these activities and issues of cost reimbursement or fair compensation to relevant parties should be considered.

Measures to be taken by law enforcement

17. Broad and strategic cooperation – Law enforcement should be encouraged to assist service providers by engaging in a broad and strategic cooperation with industry that would include conducting regular technical and legal training seminars, as well as providing feedback on investigations conducted based on complaints filed by service providers or on the intelligence gathered based on known criminal activity reported by the service providers;

18. Procedures for legally binding requests – Law enforcement should be encouraged to prepare written procedures, which include appropriate due diligence measures, for the issuing and processing of legally binding requests, and ensure that requests are carried out pursuant to the agreed procedures;

19. Training – Law enforcement should be encouraged to provide training to a designated set of their personnel on how to implement these procedures, including the manner in which records may be obtained from service providers and how to process information received, but also on

internet technologies and their impact in general as well on how to respect due process and the fundamental rights of individuals;

20. Technical resources – Law enforcement personnel responsible for cooperation with service providers should equip themselves with the necessary technical resources, including internet access, an agency-issued email address that makes the affiliated agency apparent in the address, and other technical resources to permit them to receive information securely from a service provider electronically;

21. Designated personnel and contact points – Interaction between law enforcement and service providers should be limited to trained personnel. Law enforcement should be encouraged to designate contact points for their cooperation with service providers;

22. Authority for requests – Law enforcement authorities should be encouraged to define clearly in their written procedures which law enforcement personnel can authorise what type of measures and requests to Internet service providers and how these requests can be validated/authenticated by Internet service providers;

23. Law enforcement should be encouraged to make information available to Internet service providers on their procedures and, where possible, which personnel or which nominated job positions are responsible for cooperation with Internet service providers;

24. Verification of source of request – The source of a request from law enforcement should be verifiable by service providers:

- All correspondence should include the contact name, telephone number and e-mail address of the law enforcement agent(s) seeking the records so that the service provider can contact the requesting individual if issues arise
- service providers should not be asked to correspond with an agent through the agent's personal e-mail address, but rather through an appropriate agency-provided e-mail account
- all letters should be on department letterhead, and all correspondence should include the agency's main switchboard number and website address so that service providers can take steps to verify the authenticity of requests if deemed appropriate;

25. Requests – Requests from law enforcement to service providers should be made in writing (or other legally acceptable electronic method) and leave a documentary trail. In extremely urgent cases when oral requests are acceptable, they must be immediately followed up by written (or other legally acceptable electronic method) documentation;

26. Standard request format – At the national level, and if possible internationally, law enforcement should be encouraged to standardise and structure the format used for sending requests and for responding to requests. As a minimum requests should contain the following information:

- Registration number
- Reference to legal basis
- The specific data requested
- Information to verify the source of the request;

27. Specificity and accuracy of requests – Law enforcement should be encouraged to ensure that requests sent are specific, complete and clear, and provide a sufficient level of detail to allow service providers to identify relevant data. They should be encouraged to ensure that requests are sent to the service provider that has the records. Requests for multiple and unspecified data should be avoided;

28. Law enforcement should be encouraged to provide as many facts about the investigation as possible without prejudicing the investigation or any fundamental rights in order to enable service providers to identify relevant data;

29. Law enforcement should be encouraged to provide explanations and assistance to service providers regarding non-case-related investigation techniques in order for them to understand how their cooperation will result in more efficient investigations against crime and better protection for citizens;

30. Prioritisation – Law enforcement should be encouraged to prioritise requests, especially those related to large volumes of data, to enable service providers to address the most important ones first. Prioritization is best done in a consistent manner across national law enforcement authorities and if possible internationally;

31. Appropriateness of requests – Law enforcement should be encouraged to be mindful of the cost that requests entail for service providers and give service providers sufficient response time. They should be mindful that service providers may also need to respond to requests from other law enforcement authorities, and should be encouraged to carefully monitor volumes submitted;

32. Confidentiality of data – Law enforcement should ensure the confidentiality of data received;

33. Avoid unnecessary cost and disruption of business operations – Law enforcement should be encouraged to avoid unnecessary cost and disruption of business operations of the service providers and other types of business;

34. Law enforcement should be encouraged to restrict the use of emergency contact points service to extremely urgent cases only to ensure this service is not abused;

35. Law enforcement should be encouraged to ensure that preservation orders and other provisional measures are followed up in a timely manner by disclosure orders, or the Internet service provider is informed in a timely manner that preserved data is no longer required;

36. International requests – For requests addressed to non-domestic Internet service providers, domestic law enforcement authorities should be encouraged not to direct requests directly to non-domestic Internet service providers but make use of procedures as described in international treaties, such as the Convention on Cybercrime and the network of 24/7 law enforcement points-of-contact for urgent measures, including preservation orders/requests;

37. Requests for international mutual legal assistance – Law enforcement and criminal justice authorities should be encouraged to take the necessary steps to ensure that requests for provisional measures are followed by international procedures for mutual legal assistance, or the Internet service provider is informed in a timely manner that preserved data is no longer required;

38. Coordination among law enforcement agencies – law enforcement authorities should be encouraged to coordinate their cooperation with Internet service providers and share good practices among each other nationally and internationally. Internationally they should make use of relevant international representative bodies for that purpose;

39. Criminal compliance programmes – Law enforcement should be encouraged to organise their interactions outlined above with service providers in the form of a comprehensive criminal compliance programme, and provide a description of such programme to service providers, including:

- The information necessary to contact the law enforcement designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for service provider to be able to provide documents to the criminal compliance personnel
- Other particulars specific to the law enforcement criminal compliance personnel (such as the extent that a law enforcement co-operates with multiple countries, documents to be translated into a particular language etc.);

40. Audit of the compliance system – Law enforcement authorities should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

Measures to be taken by service providers

41. Cooperation to minimize use of services for illegal purposes– Subject to applicable rights and freedoms, such as freedom of expression, privacy and other national or international laws, as well as user agreements, service providers should be encouraged to cooperate with law enforcement to help minimize the extent to which services are used for criminal activity as defined by law;

42. Service providers should be encouraged to report criminal incidents affecting the Internet service provider of which he is aware of to law enforcement. This does not oblige service providers to actively search for facts or circumstances indicating illegal activities;

43. Service providers should be encouraged to assist law enforcement with education, training and other support on their services and operations.

44. Follow up to requests from law enforcement authorities – Service providers should be encouraged to undertake all reasonable efforts to assist law enforcement in executing the request;

45. Procedures for responding to requests – Service providers should be encouraged to prepare written procedures, which include appropriate due diligence measures, for the processing of requests, and ensure that requests are followed up to pursuant to the agreed procedures;

46. Training - Service providers should be encouraged to make sure that sufficient training is provided to their personnel responsible for implementing these procedures;

47. Designated personnel and contact points – Service providers should be encouraged to designate trained personnel as contact points for cooperation with law enforcement;

48. Emergency assistance – Service providers should be encouraged to establish a means by which law enforcement may reach their criminal compliance personnel outside of normal business hours to address emergency situations. Service providers should be encouraged to provide law enforcement with relevant information for emergency assistance;

49. Resources – Service providers should be encouraged to provide contact points or personnel responsible for cooperation with law enforcement with the resources necessary to enable them to comply with requests from law enforcement;

50. Criminal compliance programmes – Service providers should be encouraged to organise their cooperation with law enforcement in the form of comprehensive criminal compliance programmes, and provide a description of such programmes to law enforcement, including:

- The information necessary to contact the providers' designated criminal compliance personnel, as well as the hours during which such personnel are available
- The information necessary for law enforcement to be able to provide documents to the criminal compliance personnel
- Other particulars specific to the providers' criminal compliance personnel (such as the extent that a service provider operates in multiple countries, documents to be translated into a particular language etc.);
- In order to allow law enforcement to make specific and appropriate requests, service providers should be encouraged to provide information on the type of services offered to users, including web links to the services and additional information as well as contact details for further information;
- Where possible, the Internet service provider should be encouraged to provide a list, on request, of which types of data could be made available for each service to law enforcement on receipt of a valid disclosure request from law enforcement accepting that not all this data will be available for every criminal investigation;

51. Verification of source of requests – Service providers should be encouraged to take steps to verify the authenticity of requests received from law enforcement to the extent possible and necessary to ensure that customer records are not disclosed to unauthorized persons;

52. Response – Service providers should be encouraged to respond to requests from law enforcement in writing (or other legally acceptable electronic method) and ensure that a documentary trail is available in relation to requests and responses accepting that this trail might not include any personal data;

53. Standard response format – Taking into account the format for requests used by law enforcement, service providers should be encouraged to standardise the format for sending information to law enforcement;

54. Service providers should be encouraged to process requests in a timely manner, in line with the written procedures they have defined and provide guidelines to law enforcement on the average delays incurred to respond to requests;

55. Validation of information sent – Service providers should be encouraged to ensure that information transmitted to law enforcement is complete, accurate and protected;

56. Confidentiality of requests – Service providers should ensure the confidentiality of requests received;

57. Explanation for information not provided – Service providers should be encouraged to provide explanations to the law enforcement authority sending a request if requests are rejected or information cannot be provided;

58. Audit of the compliance system – Service providers should be encouraged to track and audit the system of processing requests for statistical purposes, for identifying strengths and weaknesses and publish such results if appropriate;

59. Coordination among service providers – being mindful of anti-trust/competition regulations service providers should be encouraged to coordinate their cooperation with law enforcement and share good practices among each other, and make use of service provider associations for that purpose.

APPENDIX VI

OCTOPUS INTERFACE CONFERENCE ON COOPERATION AGAINST CYBERCRIME

COUNCIL OF EUROPE, STRASBOURG, FRANCE, 1-2 APRIL 2008

CONFERENCE CONCLUSIONS

More than 210 cybercrime experts from some 65 countries, international organisations and the private sector met at the Council of Europe in Strasbourg from 1 to 2 April 2008.

The Conference:

- discussed current and expected cybercrime threats and trends such as malware, identity theft and other forms of fraud, botnets and denial of service attacks, child pornography and abuse, and the implications of social networks and of technologies such as Voice over Internet Protocol and next generation networks. The Convention on Cybercrime addresses cybercrime challenges in a comprehensive manner and is very much relevant. Cybercrime is a continuously evolving phenomenon that needs to be closely monitored so that legislative and other responses can be adjusted at national and international levels as well as the private sector

- reviewed the effectiveness of cybercrime legislation. In this connection, a clear global trend was noted in that countries all over the world are strengthening their legislation using the Convention on Cybercrime as a guideline. Countries that signed this treaty were called upon to accelerate the ratification of the Convention, and other countries were encouraged to seek accession. During the Conference, Georgia signed the Convention on Cybercrime, the Dominican Republic handed over a request for accession and it was announced that the Philippines are invited to accede. It underlined the role of the Cybercrime Convention Committee (T-CY) in following the implementation of the Convention and its Protocol on Xenophobia and Racism

- discussed measures to enhance the effectiveness of international cooperation, including 24/7 points of contact and improved coordination at national levels. Countries were encouraged become a party to the Convention and to use it as the framework for international cooperation. It was agreed that the Council of Europe and the G8 High-tech Crime Subgroup maintain a joint directory of contact points

- adopted guidelines for the cooperation between law enforcement and internet service providers in the investigation of cybercrime. These guidelines can now be disseminated all over the world in order to help law enforcement and ISPs structure their cooperation. It was agreed that these guidelines should be submitted to the Cybercrime Convention Committee for consideration

- underlined the need to ensure an appropriate balance between the need to enhance security of information and communication technologies and the need to strengthen the protection of privacy, personal data, freedom of expression and other fundamental rights.

Strasbourg, 2 April 2008