Project on Cybercrime
www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Octopus Interface conference
Cooperation against cybercrime
23 – 25 March 2010
Council of Europe, Strasbourg, France

Provisional (24 April 2010)

Messages from the Octopus conference

More than 300 cybercrime experts representing countries from all continents, international organisations and the private sector met at the Council of Europe in Strasbourg from 23 to 25 March 2010 to enhance their cooperation against cybercrime. At the close of the conference participants adopted key messages aimed a guiding further action.

Participants share a common interest in pursuing the most effective approaches against the growing threat of cybercrime that societies worldwide are faced with.

Effective approaches against cybercrime comprise a wide range of innovative initiatives and actions that need to be pursued in a dynamic and pragmatic manner by public and private sector stakeholders.

At the same time, measures against cybercrime are a shared responsibility and should be based on a set of common principles to allow for clear guidance to governments and organisations, to facilitate partnerships and to ensure the political commitment to cooperate.

In this connection, participants in the conference underline that:

- For security and the protection of rights to reinforce each other, measures against cybercrime must follow principles of human rights and the rule of law.
- Security and the protection of rights is the responsibility of both public authorities and private sector organisations.
- Broadest possible implementation of existing tools and instruments will have the most effective impact on cybercrime in the most efficient manner.

Following detailed discussions, participants recommend:

- Making decision makers aware of the risks of cybercrime and encouraging them to exercise their responsibility. Indicators of political commitment include steps towards the adoption of legislation and institution building, effective international cooperation and allocation of the necessary resources.
- Implementation of the Budapest Convention on Cybercrime worldwide to sustain legislative reforms already underway in a large number of countries. Countries should consider becoming parties to make use of the international cooperation provisions of this treaty. Consensus on this treaty as a common framework of reference helps mobilise resources and create partnerships among public and private sector organisations. In this connection, the ratification of the Budapest Convention by Azerbaijan, Montenegro and Portugal prior and during the conference, and the expression of interest to accede by Argentina and other countries serve as examples to other countries.
- Establishing the Budapest Convention as the global standard goes hand in hand with strengthening the Cybercrime Convention Committee (T-CY) as a forum for information-sharing network, policy-making and standard-setting. It is encouraged to address issues

not (exhaustively) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's.

- Coherent and systematic training of law enforcement, prosecutors and judges based on good practices, concepts and materials already available.
- The establishment and strengthening of high-tech crime and cybercrime units, and incidents response and reporting teams and systems.
- The development of cooperation procedures between law enforcement agencies, CERTs/CSIRTs as well as internet service providers and the IT industry.
- Due diligence measures by ICANN, registrars and registries and accurate WHOIS information. Endorsement of the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" in line with data protection standards. ICANN is encouraged to implement these recommendations without delay.
- The many networks and initiatives against cybercrime that exist already create a dynamic and innovative environment involving a wide range of actors. Stronger networking among networks is encouraged to allow for synergies and reduce duplication. The mapping of networks exercise initiated by the Council of Europe should be continued.
- A contact list for enhanced cooperation between industry and law enforcement should be established. A proposal for a secure portal for interested parties is in preparation.
- Initiatives aimed at preventing, protecting and prosecuting the sexual exploitation and abuse of children are most valuable but require stronger support and consistency. The "Lanzarote" Convention of the Council of Europe (CETS 201) offers guidance in this respect and provides benchmarks to determine progress.
- Making use of the guidelines for law enforcement – ISP cooperation adopted at the Octopus Conference in 2008.
- Completion and broad dissemination of the results by the Council of Europe of the typology study on criminal money flows on the Internet that is currently underway.
- In order to meet the law enforcement and privacy challenges related to cloud computing existing instruments on international cooperation – such as the Data Protection Convention (CETS 108) and the Budapest Convention – need to be applied more widely and efficiently. Additional international standards on law enforcement access to data stored in the "clouds" may need to be considered. Globally trusted privacy and data protection standards and policies addressing those issues need to be put in place and the Council of Europe is encouraged to continue addressing these issues in its standard-setting activities as well as by the Global Project on Cybercrime.

Public authorities, international organisations, civil society (including non-governmental organisations) and the private sector should apply existing tools and instruments without delay and cooperate with each other to identify additional measures and responses to emerging threats and challenges.

In order to add impetus and resources to efforts against cybercrime and allow societies worldwide to make best possible use of tools, instruments, good practices and initiatives already available, a global Action Plan aimed at obtaining a clear picture of criminal justice capacities and pressing needs, mobilising resources and providing support, and assessing progress made should be launched, preferably by the United Nations and the Council of Europe in partnership with the European Union, Parties to the Budapest Convention, and other interested parties.

The results of the Octopus conference should be submitted to the United Nations Crime Congress in Salvador, Brazil (12-19 April 2010) for consideration.

Summary of plenary and workshop discussions

Panel discussion: Security and fundamental rights – what rules for the internet?

Human rights apply on the internet, including freedom of expression and privacy. The Internet plays such a role that it affects more or less all human rights and rule of law principles. Access to the internet itself is increasingly becoming a right in itself.

Attacks against the confidentiality, availability and integrity (c.i.a.) of computer data and systems and offences carried via computers are threats to fundamental rights.

At the same time, rule of law principles need to be followed to prevent arbitrary measures by public authorities, safeguards and conditions need to be established and procedural powers need to be clearly defined.

Measures against cybercrime should be designed to protect fundamental rights. Full implementation of the Budapest Convention will help Governments meet the positive obligation to protect the rights and the security of people, by criminalizing c.i.a. and other offences, by providing procedural law measures and by requiring conditions and safeguards.

Security and fundamental rights are not alternatives but go hand in hand and reinforce each other.

Security and fundamental rights on the internet are a shared responsibility. In the globalised online environment we all need to contribute to the construction of the rules that govern the Internet.

Update session

This session provided updates on:

- Developments in the European Union, including the Stockholm Programme and specific measures related to cybercrime.
- Developments at the Council of Europe, including the Cybercrime Convention Committee (T-CY), data protection, the draft MEDICRIME treaty on the counterfeiting of medicines, and the Parliamentary Assembly.
- The Internet Governance Forum (Lithuania, September 2010).
- The European Dialogue on Internet Governance (EuroDIG, Madrid, April 2010).

It furthermore provides an overview of developments related to cybercrime legislation and accession to the Budapest Convention.

This session confirmed:

- security and the protection of rights was a shared responsibility requiring consensus among key partners, political commitment to cooperate against cybercrime and the recognition of human rights and rule of law principles
- many if not most of the tools needed against cybercrime are already available
- these instruments are not necessarily globally implemented
- therefore countries need support
- a consensus should be forged among key partners to set up a global, pragmatic, inclusive mechanism to review needs, provide support and assess progress.

Workshop 1: Cybercrime training for judges and prosecutors

The challenges

The workshop commenced with an outline of the overall aim, which was to promote the implementation of the Council of Europe training concept for institutionalising training for judges and prosecutors in cybercrime matters, and identifying specific steps that can be taken in this respect taking into account existing training initiatives and good practice. Presentations were given on the following subject areas:

- The Council of Europe concept paper on cybercrime training for judges and prosecutors
- Lessons learned from Law Enforcement training
- Developing and providing access to training curricula and materials
- Establishing pilot centres for judicial training
- Towards implementation of the concept.

The following challenges were identified during a discussion session with contributions received from the audience:

- It is necessary to have the right legislation in place before training is developed. At the same time, since the development of legislation may take a long time, training could also be delivered to judges based on good practices and experience of other countries. This will help provided judges with skills and awareness and make them informed stakeholders in the legislative process
- There is a lack of common standards in evidential rules in respect of electronic evidence and admissibility
- There is a general lack of understanding of technology across the board
- Judges and prosecutors need training on technical as well as legal issues
- Defence lawyers are often excluded from existing programmes.
- There is a lack of suitable training material available
- There are many national but few international solutions
- Shortage of qualified and experienced trainers
- Too much training consists only of Powerpoint or similar presentations
- Expensive "Face to Face" training is often the only choice available
- Current training is often too academic and not practical enough

Good practices

- Examples of programmes developed in Netherlands, Portugal, France and Egypt and others including initial and in house training for judges and prosecution as well as cybercrime support infrastructures for judges
- Creation of international initiatives such as GPEN
- Existing train the trainer initiatives
- The Concept for judicial training of judges and prosecutors prepared by the Council of Europe's Project on Cybercrime and Lisbon Network which will help institutionalise such training into the curricula of judicial training institutions

The way ahead

- Awareness raising at the introductory level for all players in the Criminal Justice System
- Structured sustainable and harmonised training programmes for lawyers (prosecution and defence) as well as LE and Judges
- Cooperation with Universities and the private sector in formulating courses that meet the needs defined by players in the Criminal Justice System
- Development of a glossary of internationally accepted terms
- Combined case based scenario training for teams (police, prosecutors and judges)
- Adoption of the principles set out in the Budapest Cybercrime Convention

- Ensuring that legal, procedural and cultural differences are considered, including those between course developers, trainers and trainees
- Utilising train the trainer programmes within the overall structure
- Incorporating various learning techniques such as e-learning, distance learning, face to face activities and any others suited to specific programmes
- Recognising the importance of networking opportunities within training events.

Workshop 2: Law enforcement responsibilities

The challenge

Regulators, law enforcement agencies (LEAs) and Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs) play an important part in preventing and dealing with cyber security incidents and cyber crime. Lack or insufficient cooperation between any of these elements risks inappropriate policy responses, and prevents the control and investigation of cyber-incidents.

Internet resources, such as domain names are managed/coordinated respectively by the Internet Corporation for Assigned Names and Numbers (ICANN) and Regional Internet Registries (RIRs) and their registrars (e.g. Internet Service Providers). To obtain these resources, a registrant has to provide certain personal information to the WHOIS database. According to a recent report for ICANN, less then half of records were fully accurate (only 23% when using strict definition of accuracy).[1] Inaccuracies are also found in WHOIS of RIRs. This is of deep concern to LEAs, as it hampers their efforts to track those who use CIRs for criminal activities. Current inaccuracies are to a large extent the result of insufficient control and vetting procedures and due diligence. The arrival of IPv6 is likely to aggravate further this situation, as large amounts of IP addresses will be distributed under the current registration procedures.

Good practices

- Cyber crime units (central/regional) develop public-private cooperation and international cooperation, create instruments and procedures for investigations, and develop reporting systems.
- Public/private reporting systems crosscheck alerts at international level (European alert platform).
- LEAs and CERTs/CSIRTs and regulators play an active role in awareness raising about cyber security/crime, reporting possibilities and assistance to victims.
- Informal/trusted cooperation between LEAs and CERTs/CSIRTs.
- Contact point networks facilitate cooperation.
- The interest expressed by civil authorities to establish stronger cooperation with law enforcement, in particular with regard to training is a very positive development.
- LE concerns raised in dedicated working groups in ICANN (Government Advisory Council) and RIRs.
- Draft "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" are available and had been proposed to the Internet Corporation of Assigned Names and Numbers (ICANN) at the ICANN Seoul Meeting in October, 2009. The principle aim of these proposals is to promote a safe and secure Internet in which we minimize criminal activity on the Internet and prevent domain name abuse by:
    - Enacting enhanced due diligence procedures for ICANN's accreditation of Registrars and Registries, and Registrar's processing domain name registrations;
    - Accurate WHOIS information and availability for Law Enforcement;

[1] 'Draft Report for the Study of the Accuracy of WHOIS Registrant Contact Information', Developed by NORC at the University of Chicago for ICANN 17 January 2010, p 2.

- Transparency and accountability concerning registrars, registries, domain name resellers and third party beneficiaries.

The way ahead

Establish cybercrime units, CERTs/CSIRTs and cyber incidents/crime reporting systems. Develop cooperation procedures among the stakeholders and the private sector (ISPs).

Pending the full implementation of IPv6, preventive measures could already be implemented.

Stronger due diligence policies and measures by ICANN, registrars and registries and accurate WHOIS information with applicable data protection safeguards is recommended and the "Law Enforcement Recommended Amendments to ICANN's Registrar Accreditation Agreement (RAA) and Due Diligence Recommendations" should be endorsed. ICANN is encouraged to implement these recommendations without delay.

Workshop 3: The Budapest Convention on Cybercrime as a global framework

The challenge

The Budapest Convention on Cybercrime provides a comprehensive framework for the preparation of substantive and procedural legislation and for international cooperation against cybercrime. By March 2010 it had been ratified by 29 and signed by another 17 States. The treaty is open for accession and five countries have been invited to accede.

The challenge discussed in the workshop was whether this treaty provides a sufficient global instrument or whether a new United Nations treaty was required.

Good practices

- Recent ratifications by Azerbaijan, Montenegro and Portugal. Other countries that have signed but not yet ratified the Convention should follow their example.
- Requests for accession and invitations to accede. Several non-European countries have requested accession and have been invited to accede (e.g. Argentina, Chile, Costa Rica, Dominican Republic, Philippines). Other countries with advanced cybercrime legislation are encouraged to follow their example.
- Several countries have expressed a strong interest and are considering accession (e.g. Brazil, Indonesia, Pakistan, Sri Lanka, Senegal).
- Reforms are underway in many countries. It is estimated that more than 100 countries have made use of the Budapest Convention when drafting legislation. Examples presented in the conference included: Argentina, Azerbaijan, Botswana, Cambodia, Costa Rica, Dominican Republic, Georgia, Indonesia, Laos, Mauritius, Mexico, Moldova, Montenegro, Nigeria, Philippines, Portugal, Romania, and Senegal.
- The treaty is not static but amendments and protocols are possible to address emerging needs. In addition the Cybercrime Committee (T-CY) can adopt opinions and address recommendations to the Parties regarding the Convention's application. The Parties determine the future course of action in this respect.
- The European Union in its Stockholm Programme of December 2009 calls for global implementation of the Budapest Convention. Other organisations – such as the Organisation of American States, Asia-Pacific Economic Cooperation, Interpol and others, as well as private sector organisations have expressed their support.

The way ahead

The Budapest Convention has already made a strong impact worldwide and helped create a global trend towards stronger and more harmonised cybercrime legislation. It facilitates and strengthens the cooperation among parties to the Convention.

The workshop called on countries that have signed the treaty or been invited to accede to become full parties as soon as possible, and encouraged other countries to seek accession.

The preparation of another Treaty may have the advantage of a stronger political involvement of developing countries and may cover additional offences. However, the workshop also pointed out that a new treaty entails considerable risks such as the disruption, for several years, of reforms underway and may even result in a treaty with lower standards. In short, it would create uncertainty in the many countries that are currently putting in place cybercrime legislation and other flanking measures, inspired by the Cybercrime Convention.

Some participants referred to the need to address issues not (exhaustingly) regulated by the provisions of the Cybercrime Convention such as electronic evidence, jurisdiction and liability of ISP's. It was pointed out that the T-CY is the appropriate forum to discuss and propose additional standards.

Many participants in the workshop stressed that cybercrime should not be treated as an individual isolated topic, but that it should be dealt with in connection with other legal and practical measures concerning ICT-related issues. In a number of cases it was referred to laws on e-signature and also, in a number of cases, reference was made to personal data protection standards as incorporated in Council of Europe's Convention 108. Reference was made also to necessity of adoption of national strategies of cybersecurity and put in place mechanisms of assistants projects and cooperation especially for developing countries.

In conclusion, it was clearly established that the Cybercrime Convention is the leading standard for Cybercrime Legislation, being the most comprehensive international instrument on the matter. The many efforts undertaken by the Council of Europe and other international organisations, as well as by individual Parties to the Convention had considerably contributed to the proliferation of the Convention. Many participants in the workshop demonstrated that the legislative efforts undertaken on the basis of the text of the Convention would allow their countries to request accession within short term.

Workshop 4: Mapping networks and initiatives

The challenge

A wide range of international networks, organisations and initiatives have been established dealing with cybercrime. A mapping of networks would facilitate access to them and networking among networks. A contact list would permit public/private cooperation against cybercrime.

Specific challenges discussed include:

- In developing countries police forces do not have appropriate technology. Therefore, training for police is not helpful as they don't have the equipment to practice what they have learned. Criminals, who also do not have technology, are using internet cafés and police should be encouraged to do the same – a positive side effect is that fraudsters don't go to these cafés anymore.
- A single point of contact on cybercrime is required from law enforcement and industry.
- Learn how to deal with major global issues involving multijurisdictional issues.
- Working across the networks to facilitate the rapid exchange of information.

- Duplication of training.
- Envision the balance between different types of cybercrime, protection of fundamental rights, including the rights of minorities and xenophobia
- Too much human handling in the process of data sharing and cooperation.
- Each country has its own national legislation on how electronic evidence should be obtained and the length of time data can be kept. When it comes to industry there is a vacuum as each company seems to have its own policy.
- Law enforcement agencies in different countries are working in isolation on the same problems.

Good Practice

- Interpol with its network of National Central Reference Points from high-tech crime units
- Interpol and Europol have a secure webpage detailing the training that they are to carry out.
- The Global Prosecutor E-Crime Network – GPEN
- INHOPE
- Anti-Phishing Working Group
- Global Network Initiative
- Messaging Anti-abuse Working Group, MAAWG
- Information Security Forum
- London Action Plan
- Budapest Cybercrime Convention as the common legal framework to be used when training internationally.
- Europol has a training program, running courses, rolling out training courses, with the participation of INTERPOL. 2CENTRE is considered an interesting project.
- The Council of Europe has produced with the involvement of law enforcement and industry guidelines on law enforcement and internet service providers cooperation, which can be used in the fight against cybercrime.

Way Ahead

- Networks need to start working together, for instance criminal authorities and civil authorities have similar problems and should work together more closely.
- The Council of Europe has carried out a mapping exercise and has a resource setting out known networks.
- Automated machine processing of e-crime data prevents too much human handling.
- Contact list for industry and law enforcement. Further to an agreement between US Department of Justice and European Commission, the European Commission is proposing a secure portal to interested parties. As hosting information on an institutional website based in Europe could raise some concerns among non-European audiences. Such an initiative could be put under the umbrella of the Budapest Convention.
- Provide information about legislation and company policies to law enforcement.

Workshop 5: Capacity building / technical assistance against cybercrime

The challenge

Most countries are concerned about the growing threat of cybercrime, and many tools and instruments against cybercrime are available. However, these are not necessarily implemented in all countries and regions of the world, and nor is there necessarily longer-term sustainability built within countries. This is vital to ensure longer term success in fighting cybercrime, building and "institutionalising" capacities. Common and urgent efforts to strengthen legislative frameworks, criminal justice capacities, international cooperation and public/private cooperation, the protection of children and measures against criminal money flows on the Internet are therefore required based on tools and instruments already available, or easily adaptable. Additional resources will be required and efforts would need to be undertaken to facilitate access to development cooperation funds for measures against cybercrime.

Good practices

Good practices of technical assistance projects are already available and are evidence that impact is feasible even with limited resources. These include, for example:

- The Global Project on Cybercrime of the Council of Europe which also serves as an example of public-private cooperation.
- The cybercrime training programmes and other support offered by the United States Department of Justice.
- Activities of the United Nations Office on Drugs and Crime.
- Private sector support programme, such as the training and other forms of assistance provided by Microsoft or McAfee.
- European Union support under JPEN and ISEC programmes, including for example to the 2Centre project.
- Joint projects of the European Union and the Council of Europe, such as the Project on Cybercrime in Georgia and the planned regional Project on Cooperation against Cybercrime in South-eastern Europe.
- Joint activities, such as between the Organisation of American States, the US Department of Justice and the Council of Europe, or between ASEAN, the European Union and the Council of Europe, or between the Council of Europe and Microsoft.
- The integration of cybercrime-related activities into criminal justice or other projects can also be an effective approach.

These examples also show that the agreement on a common framework of reference, that is, the Budapest Convention, helps mobilise resources and create partnerships among public and private sector organisations.

The way ahead

All partners should support without delay the implementation of tools and instruments based on good practices and resources already available.

The launching of an Action Plan could be an effective way ahead to allow countries to stem the threat of cybercrime in an urgent manner. It could be aimed at launching a global capacity building effort and may help identify needs more clearly, mobilize resources for technical assistance and bring partners and countries together around a common agenda.

The Octopus Conference calls on the United Nations Crime Congress (Salvador, Brazil, 12-19 April 2010) to consider a recommendation to this effect.

Such an Action Plan could entail steps such as:

1. Global review of needs: the UNODC and the COE in partnership with the European Union, Parties to the Budapest Convention, and other interested parties to carry out a global review of needs of countries which will enable UN member states to get a clear picture of the state of criminal justice capacities globally, identify weak spots, gaps and pressing needs, and propose actions to address those needs.

2. This should be accompanied by a global effort to mobilize donor funding for technical assistance against cybercrime.

3. Based on the needs analysis, international and bi-lateral organizations to provide specific support to countries, among other things, to

- Strengthen legislation and its implementation
- Train law enforcement, prosecutors and judges
- Establish high-tech crime units and other specialised units
- Make international cooperation more efficient
- Join 24/7 network of contact points
- Improve public/private cooperation
- Enhance the protection of children
- Support cybercrime policies and strategies
- Awareness raising with a view to education and prevention (including reaching out to senior managers and policy-makers, civil society etc)

4. The partners of the Action Plan may consider maintaining a mechanism to assess progress made by countries. Resources are limited and development cooperation funds are not yet available for measures against cybercrime.

Workshop 6: Effective measures against the sexual exploitation and abuse of children on the internet

The Challenges

Presentations were made by representatives of the Council of Europe outlining initiatives and projects being implemented that address the issue of online child protection. It was underlined that the relevant instruments developed by the Council of Europe, namely the Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) and the Convention on Cybercrime (CETS 185) are guidelines for action and assessment of progress made by countries. During the panel discussions with representatives from ECPAT International, Cyber Peace Initiative (Egypt), OECD, Interpol, EU Safer Internet Programme and eNACSO and other participants were outlined particular issues of interest. Many of the panellists described some of the initiatives that they have undertaken by their organizations at a local and national level to deal with the issue of child sexual exploitation.

Specific examples varied from the development of a child safety initiative in Egypt to the lack of quantifiable structured data to make adequate assessment of the scope of the problem at global or national level.

Good practices

Most speakers outlined what direction and action their organizations are taking to address the issue at a national and international level. Law enforcement spoke on the issue of the use of technology to identify victims in an effort to identify potential perpetrators who prey on children.

Examples of good practices and initiatives to tackle this issue discussed were ECPAT, OECD, Cyber Peace initiatives, EU Safer Internet Programme, Interpol.

Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) provides a comprehensive set of measures and offers benchmarks for determining progress made by countries. Together with the Budapest Convention on Cybercrime this treaty represents a comprehensive guideline for countries to develop a national strategy to cope with sexual exploitation and sexual abuse of children, including criminal law measures.

Interaction between the OECD and the Council of Europe in the preparation of their respective studies is a good example of cooperation. UNICEF is also working on a study and is open to cooperation.

Other governmental organizations discussed some of the ongoing programs of work that are undertaken to empower both the law enforcement and NGO community in an effort to effectively deal with child sexual exploitation.

Other organizations are conducting studies in an effort to better recognise the scope of the problem and identify the direction needed to be effective in dealing with the issue.

The discussion then turned to the question "take down or access blocking", this brought on a very spirited exchange between several members of the audience and panel. The discussion was welcomed and progressed to a useful exchange of thought and opinions and very worthwhile.

It was agreed that blocking should be used as preventive measure and not as the ultimate solution. Preference should be given to notice and take down. However, it is crucial to find the most effective technical methods in order to avoid abuse.

The way ahead

It is evidently clear that more must be done to identify, promote and support many of the ongoing initiatives being conducted by the organizations that presented at the conference workshop. There was an overriding consensus that we are moving in the right direction but more has to be done to support these initiatives.

Specific example: More international organizations are supporting projects that aid in the identification of victim images.

There is a need for direction in the development and exchange of "best practices" on many issues pertaining to the child/victim issues.

It should be considered to engage the industry in more collaborative efforts to deal with the issue of child sexual exploitation. While it is recognized that industry has been helpful in these endeavours in the past and present, there is still a need to find better solutions and project to continue the efforts.

Better coordination among organizations and stakeholders with regard to different initiatives would help identify needs and solution. Linking of the studies in preparation by UNICEF, the OECD and the Council of Europe would serve as a good example.

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (CETS 201) should be used as guideline and – in conjunction with the Budapest Convention – as a tool for effective cooperation and criminal law measures.

Outlook: Security and privacy in the clouds

The challenge

Cloud computing, with the migration of data and services from specific computers to servers "somewhere" in the clouds, entails tremendous opportunities but also far reaching security implications that are being discussed in many fora. This session focused on the following questions:

- How are personal data protected that are stored on servers in the "clouds"; what laws govern their protection?
- What does cloud computing mean for law enforcement access to computer data and systems in the "clouds" and for jurisdiction?
- Are current regulatory frameworks regarding data protection and law enforcement sufficient?

Good practices

- The fact that the challenges related to cloud computing are discussed in multiple fora and by many organisations (such as ENISA, the Cloud Security Alliance, the OECD, the Council of Europe, industry and many others) is important in itself and will help define the questions and identify solution.
- The proposal for international standards on privacy and personal data protection adopted by the 31st meeting of data protection commissioners (Spain, November 2009) may help advance the development of common global data protection standards.
- The opening up to third countries of the Council of Europe's data protection Convention (CETS 108) and the decision to modernise this treaty offers an opportunity for countries to join an existing international instrument on data protection.
- The Budapest Convention on Cybercrime – if fully implemented and applied efficiently – offers solutions to some of the law enforcement challenges.
- The Cybercrime Convention Committee (T-CY) is currently analysing the question of trans-border law enforcement access to stored computer data.

The way ahead

- Existing instruments on cybercrime (Budapest Convention) and data protection (CETS 108) should be fully and efficiently implemented to help ensure security and privacy in the clouds.
- The Cybercrime Convention Committee to continue its study on trans-border law enforcement access and the question of jurisdiction.
- The Project on Cybercrime – in cooperation with public and private sector stakeholders could set up a working group – to carry out further research to identify good practices and possible solutions on security and privacy aspects of cloud computing.
- The preparation of additional international standards or guidelines for cloud providers and law enforcement should be considered.
- The establishment of globally trusted data protection standards and systems will need to be pursued.