

Web site: [www.coe.int/cybercrime](http://www.coe.int/cybercrime)



Strasbourg, 6 August 2010

T-CY (2010) 09

**MULTILATERAL CONSULTATION AMONG THE CONTRACTING STATES TO THE  
CONVENTION ON CYBERCRIME [CETS n° 185]**

**(The Cybercrime Convention Committee T-CY)**

**Fifth meeting  
Paris, 24-25 June 2010**

**FULL MEETING REPORT**

## Executive summary

At its fifth meeting (24 – 25 June 2010), the Cybercrime Convention Committee (T-CY):

- adopted a set of Rules of Procedure for the Bureau;
- elected Mr Markko Künnapu (Estonia) as Chair and Mr Erik Planken (the Netherlands) as Vice-Chair;
- elected Ms Nora Kaiser (Germany), Messrs Pedro Verdelho (Portugal), Andrew Fialkovskiy (Ukraine) and Ms Ioana Bogdana Albani (Romania) as members of the Bureau;
- took note that Ms Betty Shave (United States of America) will continue as member of the Bureau in accordance with the rules of procedure;
- examined the possibilities for financing the work of the Committee and instructed the Secretariat, in consultation with the Bureau, to prepare a letter from the Secretary General to the Parties to the Convention presenting the possible options on financing for their final decision;
- discussed the working methods of the Committee and decided to call on Parties to contribute to the promotion of the Convention through bilateral contacts with thirds countries;
- examined the replies of the questionnaire on Transborder access to data and instructed the Bureau to prepare terms of reference for its future standard-setting work on jurisdiction and transborder access to data and submit it to the Committee with a road map for implementation, at the earliest convenience;
- took note of the reply by the Committee of Ministers to Parliamentary Assembly Recommendation 1882(2009) “The promotion of Internet and online media services appropriate for minors” and instructed the Bureau to reflect further on possible actions of the T-CY related to the legal responsibilities of Internet Services Providers with regard to illegal content and report back to the next plenary;
- called on the United Nations Office on Drugs and Crime (UNODC) for the T-CY to be associated with its work on strengthening international co-operation on Cybercrime, including through the participation of the Committee as an International Governmental Organisation in the relevant intergovernmental expert groups of UNODC, as well as *vis-à-vis* the development of an action plan for sustainable capacity building at the international level;
- examined the possibilities of closer co-operation with the private sector, being convinced of the need thereof, and instruct the Bureau to develop concrete proposals as to how such closer co-operation can be achieved;
- welcomed the setting up by the Council of Europe of a restricted website relating to the 24/7 contact points;
- welcomed the fruitful co-operation between the Committee and the G8 High-Tech Crime Subgroup and encourage further collaboration with it with a view to strengthening the effective functioning of the network and making contact details available on secure websites;
- invited the Committee of Ministers to adopt a decision encouraging non-member states with the required legislation and proven co-operation capacity to accede to the Budapest Convention;
- invited the Committee of Ministers to mandate the T-CY, in close co-operation with the CDPC, to provide advice to the Committee of Ministers on the criteria and procedure, in conformity with article 37 of the Convention, to be followed as regards the accession of non-members to the Budapest Convention;
- decided to mark the 10<sup>th</sup> anniversary of the Budapest Convention by an appropriate event and instructed the Bureau to prepare proposals for such an event and its programme, including financing.

## **1. Opening of the meeting**

1. The Cybercrime Convention Committee (T-CY) held its fifth meeting in Paris on 24 and 25 June 2010. The meeting was chaired by the Vice-Chair, Mr Markko Künnapu (Estonia). The Chair, Ms Betty Shave (United States) was excused from participating in the meeting.

2. The Secretariat informed the Committee about the reform process in the Council of Europe and its potential impact for the work on cybercrime (see speech of Mr Jörg Polakiewicz in Appendix x).

## **2. Adoption of the agenda**

3. The agenda was adopted.

## **3. Rules of procedure for the Bureau**

4. The T-CY examined the draft Rules of Procedure for the Bureau and decided to amend the draft by increasing the number of ordinary members of the Bureau from three to four. The Rules of Procedure for the Bureau were adopted as amended.

## **4. Election of the Chair and Vice-Chair**

5. The T-CY elected Mr Markko Künnapu (Estonia) as new Chair and Mr Erik Planken (Netherlands) as Vice-Chair in accordance with the Rules of Procedure for the Bureau. The new Chair and Vice-Chair took office immediately after the meeting.

## **5. Election of the Members of the Bureau**

6. The T-CY elected four Members of the Bureau in accordance with the Rules of Procedure for the Bureau. The new Members of the Bureau are: Ms Nora Kaiser (Germany), Messrs Pedro Verdelho (Portugal), Andrew Fialkovskiy (Ukraine), and Ms Ioana Bogdana Albani (Romania). They took office immediately after the meeting.

7. The outgoing Chair, Ms. Betty Shave (United States), will continue as *de iure* member of the Bureau for the coming two years in accordance with the Rules of Procedure for the Bureau.

## **6. Financing and working methods**

8. The T-CY examined the document prepared by the Secretariat and took note of the presentation by the Secretariat concerning the financial situation of the Committee.

9. A large majority of delegations were not in a position to express their preference for either option 1 (obligatory financial contributions according to rules to be established under Article 46 (2) of the Convention) or option 2 (financing through the creation of an enlarged partial agreement covering cybercrime and Internet security issues). Those delegations expressing their preference for option 1 or option 2 were almost equally divided.

10. A number of delegations, referring to the unique position of the Convention and the work of the T-CY globally on policy-making and standard-setting in the field of cybercrime, underlined the importance of providing for the funding of the T-CY through the ordinary budget of the Council of Europe as a political signal, that the Council of Europe is attaching priority to the fight against cybercrime.

11. The Committee decided to instruct the Secretariat, in consultation with the Bureau, to prepare a letter from the Secretary General to the Parties to the Convention presenting options 1 and 2 on financing for their final decision.

12. Moreover, the Committee welcomed the Secretary General's decision to declare Internet security and Cybercrime as priorities for the Council of Europe. It decided to invite the Committee of Ministers and the Secretary General to provide the T-CY with adequate financial and human resources, enabling the Committee to fulfil its important functions properly.

13. While awaiting a decision on the modalities for future financing and underlining the need for the Council of Europe to provide through its ordinary budget for financial resources for the work of the Committee, the Committee called on Parties able to do so to provide voluntary contributions.

14. As regards working methods of the Committee, the T-CY discussed how best to assist the Council of Europe in promoting the Convention. It was agreed that Parties should promote the Convention in their bilateral contacts with third countries.

### **7. and 8. Transborder access to data and jurisdiction on the Internet and related matters**

15. The T-CY took note of the presentation provided by the Secretariat concerning the questionnaire on transborder access to data and examined the replies to the questionnaire. In this context, the Committee discussed the practical applications of Article 32 (b) of the Convention and their legal implications. With this in mind one delegation made the observation that the main problem of transborder access to data and data flows is not so much the technical or legal challenges involved, as these can generally be overcome, but the underlying – essentially political – problem of sovereignty of states and the implied breach thereof, whenever authorities of one state effectively operate in the jurisdiction of another state without having obtained the necessary authorisations.

16. In this context some delegations expressed their concern that it was important to carefully circumscribe the right for Parties to transborder access to data in order to avoid such access being abused for espionage purposes.

17. The T-CY continues its discussions on jurisdiction on the Internet and related matters, in particular with regard to problems incurred in cooperation between law enforcement authorities and Internet Service Providers (ISP), as well as the effects of “cloud computing”.

18. The Committee welcomed the presentation on cybercrime and jurisdiction by the delegation of the Netherlands.

19. The Committee instructed the Bureau to prepare terms of reference for its future work on standard-setting in the closely related areas of jurisdiction and transborder access to data and submit it to the Committee. The draft terms of reference should also include a road map for implementation.

### **9. Responsibilities of Internet Service Providers (ISP)\***

20. The T-CY took note of the comments of the Committee (prepared by the Bureau) and the Committee of Ministers' reply to Parliamentary Assembly Recommendation 1882 (2009) entitled “The promotion of Internet and online media services appropriate for minors”.

21. The Committee instructed the Bureau to reflect further on possible actions of the T-CY related to the legal responsibilities of Internet Service Providers with regard to illegal content and report back to the next plenary.

### **10. Cybercrime and data protection: Presentation by Ms Vanna Palumbo of the Italian Data Protection Authority**

22. The T-CY took note of the presentation by Ms Palumbo about work currently being undertaken on law enforcement and privacy by the “Working Party on Police and Justice”. This Working Party has been mandated by the European Conference of data protection authorities to monitor and examine the developments in the area of police and law enforcement to face the growing challenges for the

protection of individuals with regard to the processing of their personal data. The importance of having adequate data protection standards when implementing the Convention on Cybercrime was emphasised.

#### **11. International co-operation on cybercrime related matters between states, international organisations and the private sector: Relations with other organisations (UN, G8, EU, OECD)**

23. The Secretariat informed the Committee about the outcome concerning cybercrime of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice, which took place in Salvador de Bahia, Brazil, from 12 - 19 April 2010, and the UNODC May meeting in Vienna, from the Council of Europe perspective.

24. Representatives of the aforementioned observer organisations and institutions (with the exception of the EU which was not present) informed the Committee about relevant activities.

25. The Committee called on the United Nations Office on Drugs and Crime (UNODC) to associate the T-CY with its ongoing and planned work on strengthening international cooperation on cybercrime. The representative of the UNODC explained that the Council of Europe would be entitled to representation as an International Governmental Organisation (IGO) in the relevant inter-governmental expert groups of UNODC as well as vis-à-vis the development of an action plan for sustainable capacity building at international level.

26. As regards co-operation with the private sector, the T-CY underlined the importance of closer co-operation and instructed the Bureau to develop concrete proposals as to how such closer cooperation can be achieved.

#### **12. The merger and harmonisation of lists of contact points\***

27. The T-CY took note of the information provided by the Secretariat on how, in accordance with the decisions of the T-CY at its Fourth meeting on 12 and 13 March 2009, the Bureau of the T-CY has, through the Secretariat, conducted discussions with the G8 concerning a possible partial merger of the lists of contact points on cybercrime as part of the collaboration between the T-CY and the G8 on the 24/7 Network.

28. The Committee noted that a complete merger of lists faces difficulties because of a wider scope of functions of 24/7 contact points under the Cybercrime Convention. Nevertheless, the Committee welcomed the fruitful cooperation with the G8 High-Tech Crime Subgroup and encouraged further collaboration with it, aiming at strengthening the effective functioning of the network and making contact details available on secure websites.

29. The Secretariat informed about the new website [www.coe.int/tcy](http://www.coe.int/tcy) which now contains a restricted area designed to host contact details concerning the 24/7 network. These data will consequently be removed from the Treaty Office website (except the general name of ministry/entity and address if available).

30. The delegation of Italy informed the Committee about a new secure website which is being developed by the Italian authorities in cooperation with the EU and the G8 for hosting cybercrime contact lists. In the future, the lists of the 24/7 network of the Council of Europe could possibly also be hosted on this site.

#### **13. Situation concerning accessions to the Convention and its Additional Protocol**

31. The T-CY took note of the information provided by the Secretariat on the state of accession to the Budapest Convention and its Additional Protocol. Delegations representing states that are not yet parties to the Budapest Convention and/or its additional protocol provided information about ongoing ratification or accession procedures.

**14. Development of criteria to be applied by the T-CY for recommending accession of non-member states to the Convention to the Committee of Ministers\***

32. The T-CY examined the discussion paper prepared by the Secretariat on modalities of accession by third countries to the Budapest Convention (doc. T-CY(2010) 06).

33. On the basis of its discussions, the T-CY decided to invite the Committee of Ministers to adopt a decision encouraging non-member states with the required legislation and proven cooperation capacity to accede to the Convention. It further invited the Committee of Ministers to mandate the T-CY to provide – in close cooperation with the CDPC – advice to the Committee of Ministers on the criteria and procedure to be followed as regards the accession of non-members to the Convention. The Committee underlined that such criteria and procedures should respect Article 37 of the Convention.

**15. 10th anniversary of the Convention**

34. 23 November 2011 will mark the 10th anniversary of the Budapest Convention. The T-CY decided to mark the anniversary by an appropriate event. Some delegations proposed to produce a publication on the Convention as part of such an event celebrating the anniversary. The Committee instructed the Bureau to prepare proposals for an event and its possible programme. The proposals should look into the financing of an event.

**16. Any other business**

35. No issues were raised under this item.

**17. Next meeting of the Cybercrime Convention Committee (T-CY)**

36. The Committee decided to set a date for its next plenary meeting in 2011 through a written procedure in consultation with the Bureau.

\* \* \* \*

## APPENDIX I

### Rules of Procedure for the Bureau (T-CY (2010) 04)

#### Composition, election, functions and competences of the Bureau

##### Article 1. Composition of the Bureau

1. The Bureau shall be composed of the Chair, the Vice-Chair of the Committee, together with four elected members and the outgoing Chair who may remain a member *de iure* of the Bureau during the first mandate of the new Chair. The other members shall be elected from among the representatives on the Committee. The Bureau is elected for a period of two years. The members, including the Chair and Vice-Chair, shall be eligible for re-election once.
2. The Vice-Chair shall replace the Chair, if the latter is absent or otherwise unable to preside over the meeting. If the Vice-Chair is absent, the Chair shall be replaced by another member of the Bureau, appointed by the latter.
3. If a member of the Bureau ceases to be a member of the Committee or resigns his/her office before its normal expiry, the Committee may elect a successor for the remainder of the term of that office.
4. If a member is not able to participate in a meeting of the Bureau, he/she may appoint an ad hoc replacement.

##### Article 2. Election of the Bureau

1. Election of the Chair and the Vice-Chair shall require a two-thirds majority at the first ballot and a simple majority at the second ballot. The election shall be held by a show of hands, unless a member of the Committee requests a secret ballot.
2. Other members of the Bureau shall be elected in the same manner as the Chair and Vice-Chair. They shall be elected immediately after the Chair and the Vice-Chair in accordance with an equitable distribution of posts, taking into account in particular, geographical distribution, gender balance and legal systems.

##### Article 3. Meetings of the Bureau

Except where otherwise decided by the Bureau, it shall meet in closed session.

##### Article 4. Functions of the Bureau

The Bureau shall direct the work of the Committee between plenary meetings, and in particular:

- a. prepare preliminary draft legal instruments and draft opinions;
- b. prepare and approve opinions requested by Council of Europe bodies;

- c. prepare reports taking into account of the comments of the Committee delegations, where possible, unless the report is urgent;
- d. prepare the programme of activities and propose priorities to the Committee for future work according to the Committee' working programme with a suggested timetable;
- e. review the agenda of the plenary meeting and propose the way the Committee's business should be dealt with (for example, drafting the order of business, identifying issues of particular importance, etc);
- f. invite external guest speakers, where appropriate;
- g. appoint experts to carry out specific activities;
- h. make appointments to other Council of Europe bodies;
- i. report back to the Committee on its activities between the plenary meetings;
- j. deal with any other matter specifically delegated to it by the Committee.

**Article 5. Decisions of the Bureau**

Before taking a decision, unless the matter has been specifically delegated to it by the Committee in accordance with Article 4 (j), the Bureau shall consult the members of the Committee and take their observations into account. When the Bureau exercises the powers of the Committee, its decisions shall be taken by consensus. Where there is disagreement, it shall submit its draft decision to the Committee.

\* \* \* \*



## APPENDIX II

### AGENDA

1. Opening of the meeting  
Speech by the Secretary General of  
the Council of Europe
2. Adoption of the agenda  
T-CY (2010) 02  
T-CY (2010) 02 ann
3. Rules of procedure for the Bureau  
T-CY (2010) 04
4. Election of the Chair and Vice-Chair
5. Election of the Members of the Bureau
6. Financing and working methods  
T-CY (2010) 03
7. Transborder access to data  
T-CY (2010) 01  
T-CY (2010) 05  
restricted documents distributed by  
mail
8. Jurisdiction on the Internet and related matters
9. Responsibilities of Internet Service Providers  
(ISP)  
Recommendation 1882(2009)  
T-CY (2010) 08
10. Cybercrime and data protection:  
Presentation by Ms Palumbo (Data Protection  
Commissioner, Italy)  
Draft Recommendations  
Draft decision supervision policy  
Draft annual report for the year 2009 -  
Working Party on Police and Justice  
Draft model clause - Bilateral Agreements -  
Working Party on Police and Justice  
Resolution of the Spring  
Conference 2010 of the European  
Data Protection Commissioners  
T-PD-BUR (2010) 03
11. International co-operation on cybercrime  
related matters between states, international  
organisations and the private sector: Relations  
with other organisations (UN, G8, EU)

12. The merger and harmonisation of lists of contact points

13. Situation concerning accessions to the Convention and its Additional Protocol

Treaty Office's list  
T-CY (2010) 07

14. Modalities of accession by non-member States to the Convention to the Committee of Ministers

T-CY (2010) 06

15. 10<sup>th</sup> anniversary of the Convention

16. Any other business

17. Next meeting of the Cybercrime Convention Committee (T-CY)

\* \* \* \*

**APPENDIX III  
LIST OF PARTICIPANTS**

**BUREAU MEMBERS / MEMBRES DU BUREAU**

**Chair of the Committee / Présidente du Comité :**

**Ms Betty SHAVE (United States of America / Etats-Unis d'Amérique),** apologised / *excusée*

**Vice-Chair of the Committee / Vice-Président du Comité :**

**Mr Markko KÜNNAPU (Estonia / Estonie)**

Adviser, Criminal Police Department, Ministry of Justice

**Members / Membres :**

**Ms Nora KAISER (Germany / Allemagne)**

Deputy Head of Division, Federal Ministry of Justice

**Mr Erik PLANKEN (The Netherlands / Pays-Bas)**

Ministerie van Justitie, DGRR, Directie Rechtshandhaving en Criminaliteitsbestrijding,  
Afdeling Criminaliteit en Veiligheid

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

**ALBANIA / ALBANIE**

**ARMENIA / ARMENIE**

**AZERBAĪJAN / AZERBAIDJAN**

Mr Bakhtiyar N. MAMMADOV

Head of Legal and Human Resources Department,  
Ministry of Communications and Information Technologies

**BOSNIA AND HERZEGOVINA / BOSNIE-HERZEGOVINE**

Mr Tomislav ĆURIĆ

Expert Adviser in Department for Combating Organized Crime and Corruption, Ministry of Security

**BULGARIA / BULGARIE**

**CROATIA / CROATIE**

Mr Josip ŽUVELA

Police Adviser, Economic Crime and Corruption Department, Ministry of the Interior

**CYPRUS / CHYPRE**

Ms Polina EFTHIVOULOU-EFTHIMIOU

Counsel of the Republic A', Law office of the Republic of Cyprus

**DENMARK / DANEMARK,** apologised / *excusé*

**ESTONIA / ESTONIE**

Mr Markko KÜNNAPU

Adviser, Criminal Police Department, Ministry of Justice

**FINLAND / FINLANDE**, apologised / *excusée*

**FRANCE**

Mme Delphine GAY

Capitaine de Police, Groupe Relations Internationales, Formations et Synthèses, OCLCTIC

Office Centrale de Lutte contre la Cybercriminalité de la Direction de la Police Judiciaire

**GERMANY / ALLEMAGNE**

Ms Nora KAISER

Deputy Head of Division, Federal Ministry of Justice

**HUNGARY / HONGRIE**

Ms Eszter VICZKO

Legal adviser, Criminal Law Department, Ministry of Public Administration and Justice,

**ICELAND / ISLANDE**

**ITALY / ITALIE**

Dott. Sergio STARO

Primo Dirigente della Polizia di Stato, Ministero dell'Interno, Servizio Polizia Postale e delle Comunicazioni, Relazioni Internazionali

Dott. Vittorio STANCA

Sostituto Commissario della Polizia di Stato, Ministero dell'Interno, Servizio Polizia Postale e delle Comunicazioni, Relazioni Internazionali

**LATVIA / LETTONIE**

Mr Aleksandrs BUKO

Head of Cybercrime enforcement unit

**LITHUANIA / LITHUANIE**, apologised / *excusée*

**MOLDOVA / MOLDAVIE**

Mr Veaceslav SOLTAN

Chief Prosecutor, Head of Section on Informational Technologies and Investigation, Informational Crime, General Prosecutor Office

**MONTENEGRO**, apologised / *excusé*

**NETHERLANDS / PAYS-BAS**

Mr Erik PLANKEN

Ministerie van Justitie, DGRR, Directie Rechtshandhaving en Criminaliteitsbestrijding, Afdeling Criminaliteit en Veiligheid

Mr Jean Luc LUIJS

Policy Advisor, Law enforcement, Ministry of Justice

Mr August NIELAND

Legislative Advisor, Ministry of Justice

**NORWAY / NORVEGE**

Mr Magnar AUKRUST

Deputy Director General in the Police Department, Ministry of Justice and the Police

Mr Eirik TRØNNES HANSEN  
Police Prosecutor, Cyber Crime Investigation Section, High-Tech Crime Department, National Criminal  
Investigation Service

**PORTUGAL**

Mr Pedro VERDELHO  
Public Prosecutor, Centro de Estudos Judiciários

Mr João MELO  
Public prosecutor in DCIAP – PGR, DCIAP

**ROMANIA / ROUMANIE**

Ms Raluca SIMION  
Legal Adviser , Directorate International Law and Treaties, Ministry of Justice and Citizens' Liberties

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 Organized Crime and Terrorism,

**SERBIA / SERBIE**

**SLOVAKIA / SLOVAQUIE**

**SLOVENIA / SLOVENIE**

**SPAIN / ESPAGNE**, apologised / *excusée*

**“THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA” /  
“L’EX-REPUBLIQUE YOUGOLSAVE DE MACEDOINE”**

Mr Igroche KARAFILOVSKI  
Head of the Sector for regulation and system development, Office for Prevention of Money Laundering and  
Financing Terrorism

**UKRAINE**

Mr Valentyn PETROV  
Expert of the Security Service of Ukraine

Mr Andrew FIALKOVSKYI  
Advisor for National Security Council

**UNITED STATES OF AMERICA / ETATS-UNIS D’AMÉRIQUE**

Mr Thomas DUKES  
Trial Attorney, Computer Crime and Intellectual Property Section, Criminal Division  
U.S. Department of Justice

**OTHER PARTICIPANTS / AUTRES PARTICIPANTS**

**ANDORRA / ANDORRE**

**AUSTRIA / AUTRICHE**

**BELGIUM / BELGIQUE**

**CANADA**

Mr Gareth SANSOM  
Director, Technology & Analysis, Criminal Law Policy Section, Ministry of Justice

**CHILE / CHILI**

Mr Jorge BIDAL  
Diplomat, Ministry of Foreign Affairs, Embassy of Chile in Paris

**COSTA RICA**

**CZECH REPUBLIC / REPUBLIQUE TCHEQU**, apologised / *excusée*

**DOMINICAN REPUBLIC / REPUBLIQUE DOMINICAINE**

**GEORGIA / GEORGIE**

**GREECE / GRECE**

**IRELAND / IRLANDE**

**JAPAN / JAPON**

Mr Kazuhisa KONDO  
Attorney, International Organized Crime Division, Foreign Policy Bureau, Ministry of Foreign Affairs

Mr Keiichi TANIYAMA  
Assistant Director, Cybercrime Division, Community Safety Bureau, National Police Agency

Mr Hiroyuki MINAMI  
Consul (Attorney), Consulate-General of Japan at Strasbourg, Consulate-General of Japan

**LIECHTENSTEIN**, apologised / *excusé*

**LUXEMBOURG**

M. Laurent THYES  
Attaché de Gouvernement, Direction Pénale et judiciaire, Ministère de la Justice,

**MALTA / MALTE**

**MEXICO / MEXIQUE**

Mr Raúl VILLEGAS LASTRA  
Coordinator of Cybersecurity Efforts, Center for Research and National Security, Ministry of the Interior

Ms Corina CADENA  
Affaires Juridiques, Ambassade du Mexique en France

**MONACO**

**PHILIPPINES**

**POLAND / POLOGNE**

**RUSSIAN FEDERATION / FEDERATION DE RUSSIE**

M. Igor KONDRATSKIY  
Conseiller de l'Ambassade Russe à Paris

**SAN MARINO / SAINT MARIN**

**SOUTH AFRICA / AFRIQUE DU SUD**

**SWEDEN / SUEDE**

**SWITZERLAND / SUISSE**

M. Andrea CANDRIAN

Département fédéral de justice et police, Office fédéral de la justice, Unité droit pénal international

M. Adrian KOSTER

Analyste et Juriste, Service de renseignement de la Confédération, Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI

**TURKEY / TURQUIE**, apologised / excusée

**UNITED KINGDOM / Royaume-Uni**

Mr Justin MILLAR

Head of Computer Crime, OFCU, Home Office

**EUROPEAN COMMITTEE ON CRIME PROBLEMS**

**/ COMITE EUROPEEN POUR LES PROBLEMES CRIMINELS (CDPC)**

**STEERING COMMITTEE ON THE MEDIA AND NEW COMMUNICATION SERVICES**

**/ COMITE DIRECTEUR SUR LES MEDIAS ET LES NOUVEAUX SERVICES DE COMMUNICATION (CDMC)**

**INTERNATIONAL TELECOMMUNICATION UNION (ITU)**

**/ UNION INTERNATIONALE DES TELECOMMUNICATIONS (UTI)**

**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)**

**UNITED NATIONS OFFICE ON DRUGS AND CRIME (UNODC)**

**/ OFFICE DES NATIONS UNIES CONTRE LA DROGUE ET LE CRIME (UNODC)**

Ms Gillian MURRAY

Officer in Charge, Conference Support Section, Focal Point for Cybercrime, Organized Crime and Illicit Trafficking Branch, Vienna International Centre

**EUROPEAN COMMISSION / COMMISSION EUROPEENNE**, apologised / excusée

**EUROPOL**

**INTERPOL**

**ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT**

**/ ORGANISATION DE COOPERATION ET DE DEVELOPPEMENT ECONOMIQUES**

Mr Laurent BERNAT

Administrator, Directorate for Science Technology, Information, Computer, and Consumers Policy Division

**G8**

Mr Christopher PAINTER

Chair of G 8 Roma/Lyon Group - High Technology Crime Subgroup

**SPEAKERS / INTERVENANTS**

Mrs Vanna PALUMBO

Head of the International Department, Italian Authority Data Protection

Mr Henrik KASPERSEN

Emeritus Professor, Vrijeuniversiteit Amsterdam

**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  
DG-HL***

Mr Jörg POLAKIEWICZ, Secretary to the T-CY, Head of Law Reform Department

Mr Kristian BARTHOLIN, Co-Secretary to the T-CY, Law Reform Department

Mr Alexander SEGER, Head of Economic Crime Division

Mr Lee HIBBARD, Coordinator for Internet Governance and Information Society

Ms Evgenia GIAKOUMOPOULOS, Study visitor

Ms Anna LE VALLOIS, Assistant, Law Reform Department

**INTERPRETERS / INTERPRETES**

Mme Geneviève MC KINNON

Mme Marie-Madeleine RIGAS

M. Robert WOLFENSTEIN

\* \* \* \*



## APPENDIX IV

### T-CY Opening speech Paris 24 June Jörg Polakiewicz, Secretary of the T-CY

I would like to welcome all of you to the Paris office of the Council of Europe, in particular those of you who have come from far away, the representatives from Canada, Japan, Mexico and the USA. I am confident that we may have meetings in other parts of the world soon.

We are at a **defining moment** in our common effort to combat all forms of cybercrime. This can only be a global effort. I am pleased to welcome representatives from the UN, EU, OECD and G8, with all of whom we have already and shall co-operate closely.

I would like to give a brief overview of relevant Council of Europe activities and highlight the main subjects of our meeting today and tomorrow.

#### **Council of Europe activities beyond the Budapest Convention**

The Committee of Ministers adopted on 26 May a “**declaration on enhanced participation of member states in Internet governance matters**”. The Committee of Ministers recognised the role of the Governmental Advisory Committee (GAC) within ICANN, the Internet Corporation for Assigned Names and Numbers. All Council of Europe member states are encouraged to actively participate in GAC and the Secretary General is invited to make arrangements for the Council of Europe to participate as an observer in GAC’s activities. All this with the aim to ensure that international human rights law and other public policy objectives are taken into account in the activities of ICANN.

Last week, the Committee of Ministers adopted a **reply to Parliamentary Assembly Recommendation 1882 (2009) “The promotion of Internet and online media services appropriate for minors”**. The Committee of Ministers noted in particular the call for greater legal responsibilities for Internet service providers with regard to illegal content and invited “the relevant committees to engage in reflection on this matter.” This will indeed be one the topics of this meeting.

The **Steering Committee on Media and New Communication Services (CDMC)** is currently preparing a draft declaration on the Digital agenda for Europe, a draft declaration on network neutrality, a draft declaration on management of the Internet protocol address resources in the public interest as well as dealing with critical internet resources. I am happy that the new coordinator for information society and Internet governance Lee Hibbard is with us.

Our **data protection committee (T-PD)** finalised a draft Committee of Ministers’ recommendation on profiling, which would cover profiling used by public (law enforcement) and private authorities (behavioural advertising).

#### **Activities centred around the 2001 Budapest Convention**

Where do we stand with the Budapest Convention? We have at present

- 30 ratifications: European countries and the USA. Since our last meeting in March 2009, Azerbaijan, Moldova, Montenegro, Portugal, Spain and Serbia have ratified.
- 16 signatures: European countries, Canada, Japan and South Africa.
- 5 countries invited to accede: Chile, Costa Rica, Dominican Republic, Mexico, Philippines.
- 2 requests for accession from Argentina and Australia. Invitations are expected by September.

Moreover, the Convention is used as a guideline, reference standard or model law in more than 100 countries.

The “**Salvador declaration**”, adopted at the UN Crime Congress (12-19 April 2010), calls for a:

- worldwide capacity-building effort, “in order to deal with cybercrime, including the prevention, detection, investigation and prosecution of such crime in all its forms”;
- “expert group to conduct a comprehensive study ... and to propose new national and international legal or other responses to cybercrime.”

The Council of Europe stands ready to participate actively in both.

As regards **capacity-building**, we have the Project on cybercrime (since 2006). Phase 1 had been completed in February 2009. Phase 2 was launched in March 2009. The overall objective is to promote implementation of the Budapest Convention and related international standards. Activities focus on:

- legislation and policies;
- international cooperation;
- law enforcement – service provider co-operation in the investigation of cybercrime;
- training of judges and prosecutors;
- data protection and privacy;
- exploitation of children and trafficking in human beings.

As regards **follow-up to the Budapest Convention**, consultations of Parties have regularly taken place since 2006 within the T-CY. The Convention and its explanatory report describe the T-CY as, “a framework for the Parties to consult regarding implementation of the Convention, legal, policy or technological developments and the possibility of supplementing or amending the Convention”. It is a treaty-based mechanism whose terms of reference result directly from the Convention (and not from Committee of Ministers’ decisions).

The Convention’s explanatory report stresses two important points. Firstly, the flexibility of the follow-up procedure which allows the association of all parties to the Convention, including non-member States on an equal footing basis – this is certainly a strength. Secondly, the importance to associate the views of interested parties, including law enforcement, non-governmental and private sector organisations.

During the last Octopus conference in March 2010, participants stressed that making the Budapest Convention a truly global instrument required a strengthening of the T-CY.

#### **What should be the T-CY priorities?**

If we want the convention to remain relevant, we shall have to adapt to changes both in technology and the nature of threats which have taken place since 2001. The T-CY should be more than a mere information-sharing network. We should strengthen its standard-setting and policy-making roles.

Faced with technological development, there is a need to develop further standards, soft-law standards as well as, if appropriate, additional protocols. Parties need guidance on application and implementation of the Convention’s relatively complex provisions, which do not exhaustively address all issues. The 2010 Octopus conference mentioned as examples electronic evidence, jurisdiction and ISP liability. In fact the latter two are already on our agenda. Moreover, Parties which come increasingly from beyond Europe and North America, will be less familiar with the existing Council of Europe treaty frameworks for international cooperation in criminal matters.

Conclusions of the T-CY may take the form of opinions, guidelines or recommendations to the parties. These are typically soft law instruments. If the parties agree, some may qualify as “authoritative interpretations” under the 1969 Vienna Convention on the Law of Treaties. Already in 2006, the T-CY agreed that cell phones qualify as computer systems and thus enjoy protection under the Convention.

Reinforcing the T-CY's activities does not come for free. So far, cybercrime-related activities have been financed by the Council of Europe's ordinary budget and, as regards the project on cybercrime, through voluntary contributions. The current situation is unsatisfactory for several reasons:

- a lack of sufficient resources; in fact both the T-CY and the project are currently underfinanced;
- non-member states do not contribute, except on a voluntary basis;
- fragmented activities.

The scope for increased funding under the Council of Europe's ordinary budget is unfortunately limited.

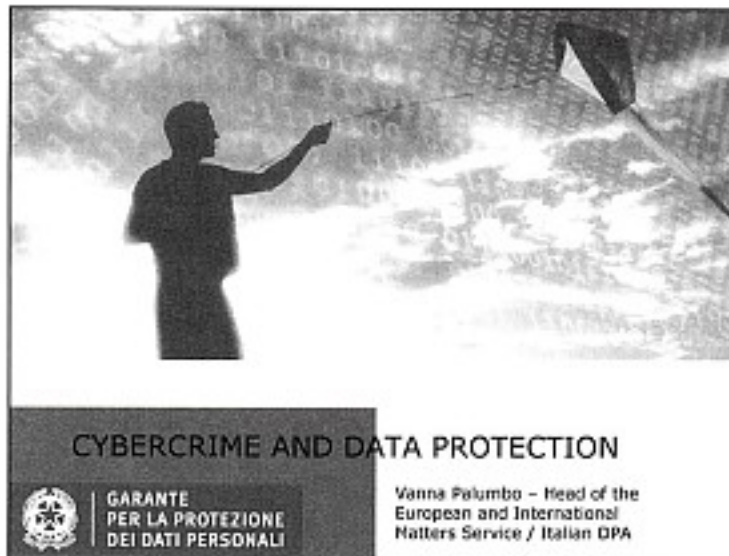
This brings me to my final point, the **reform process within the Council of Europe**. The new Secretary General, Mr Torbjørn Jagland, has formulated his political priorities. He wants to transform the Council of Europe into a more focused and political organisation and to revitalise it as a political body. The Council of Europe should concentrate on fewer projects, selected on the basis of added value and impact. The main priority is currently the reform of the European Court of Human Rights following the Interlaken conference and EU accession to the ECHR. "Internet security and cybercrime" are identified as priorities for 2011, but this does not mean that there is automatically more money available.

Facing a challenge of global dimensions, we need sustained financing within a flexible structure which can associate not only member and non member states, but also other international actors active in this field, in particular the EU and the UN, as well as the private sector.

As the French say: "l'union fait la force!"

## APPENDIX V

### Presentation of Mrs Vanna Palumbo, Head of the International Department, Italian Authority Data Protection



GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in Europe

- A comprehensive legal framework for the processing of data, both in the private and in the public sector, including processing of personal data by police and judicial authorities (Convention 108/1981 – Council of Europe)
  - Supplemented by specific principles regulating the use of personal data in the police sector (Recommendation 87(15) of 1987)

HOWEVER: Many exceptions along with sector-related recommendations that are not directly binding → which may account for diverging domestic provisions

2




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in Europe

- Benchmark for the definition of data protection principles in the development of instruments or information system for enhancing security and police cooperation at EU level in the perspective of a borderless Europe (Schengen SIS, Europol, Pruem)
- The third (and last) evaluation of 2002 proved particularly interesting also with a view to considering principles contained in MLA Conventions and Cybercrime Convention (Article 28 and relevant recitals)

3




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in Europe

- Decision to update the Recommendation (T-PD Committee) and also draft a new protocol in order to make the basic principles more effective, in particular considering the impact of new technologies

4




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in the EU

- Before the entry into force of the Lisbon Treaty, which has also affirmed right to privacy and data protection as fundamental rights, data protection principles introduced on an harmonized base at EU level with the adoption of Directive 95/46/EC were not applicable to matters not covered by Community law due to division into pillars of the competences → in practice leaving outside all data processing for LEAs and judicial activities.

5




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in the EU - The "3rd Pillar"

- No harmonised set of specific rules
- DP principles laid down in **sector-specific instruments**


6

 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in III Pillar – Availability Principle

- Subsequent implementation of The Hague Programme → Need for an appropriate set of principles to accompany the definition of enhanced mechanisms for police and judicial cooperation and data exchange, such as those based on the principle of availability


7

 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Data Protection in the III Pillar – Supervision and Monitoring by DPAs

- **Many initiatives** in Third Pillar sector, **lack of coordination** (Council, Community, Parliament)
- **The Data protection authorities asked for major changes** to define an institutional framework for data protection ensuring a high level of protection and effective supervision at national level along with appropriate mechanisms for stimulating coordination, exchange of views and supervisory activities between national DPAs (only partially achieved with the adoption of the Framework Decision 2008/977/JHA).
- To this end they decided to give new life to their activities in the field

8




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### Working Party on Police and Justice Background

- The **WPPJ** started its activities in **June 2007** under Italian chairmanship to fulfil the mandate committed by the 2007 Spring Conference of European data protection authorities.
- **Mandate** of this Group: proactively monitoring the developments in data protection as for the so-called "Third Pillar".

9




GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### WPPJ's Membership and Activity

- The WPPJ is composed by a representative from each of the national Data protection authorities of the European States members of the Spring Conference plus the EDPS
- Working method: mutual co-ordination and proactivity; close relationships with European data protection authorities;
- The mutual collaboration between the WPPJ and Article 29 WP has also proven especially fruitful → Joint opinion on draft framework decision on the so-called "**European PNR**" plus several other documents (Contribution on Future of Privacy Consultation; SWIFT case)

10




 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## WPPJ's Activity

- Major efforts were made by the WPPJ to have its voice heard in the appropriate forums, starting from the European Parliament;
- WPPJ put forward proposals and solutions and did not limit itself to statements of principle;
- Special importance should be attached to the work carried out in respect of the draft framework Decision on data protection in the III pillar;
- Assessment of implementing measures of the Prüm Treaty, which led the WPPJ to develop two position papers containing practical guidance and recommendations;
- More recently the contribution for a joint document on the Future of Privacy asks for a comprehensive set of rules while reaffirming the necessity for tailor-made rules in the field of police and judicial activities.


11

 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

## WPPJ's Activity – Bilateral Agreements with Third Countries

- Resolution by 2009 Spring Conference: WPPJ to develop "data protection clause" to be incorporated in future agreements.
- Survey completed in October 2009, concerning data protection aspects of bilateral agreements concluded with non-European countries in the area of police and judicial co-operation
- WPPJ developed (April 2010) model data protection clauses (shorter and longer versions) based on CoE's Convention 108/81 and EU directive 95/46


12

 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### WPPJ's Activity – Cybercrime Convention

- Survey completed in October 2009, concerning national implementing measures to transpose CoE's cybercrime convention
- Shortcomings were highlighted, guidance by WPPJ was considered helpful
- Set of Recommendations was adopted (April 2010) by WPPJ (for Member States that have not yet implemented the Convention; for monitoring national implementation)

13

 GARANTE  
PER LA PROTEZIONE  
DEI DATI PERSONALI

### WPPJ's Future Work

- Focus on implementation of surveillance techniques and the risks related to data mining and profiling by law enforcement bodies (including border controls and aviation security issues).
- Enhance activities as regards monitoring justice-related developments (as outlined in the Stockholm Programme)
- Develop guidance for implementation of the Framework Decision on DP in III Pillar
- Risk assessment exercise undertaken via the "Catalogue on Supervision and Co-operation" to lay down mid-term supervision policy at European level
- Improve awareness-raising (see also Action Plan by European Commission and many initiatives in law enforcement area)

14

## APPENDIX VI

### Presentation outline of Messrs Planken and Nieland from the Netherlands Delegation

#### Cybercrime investigations and state sovereignty – some thoughts on the way forward

##### Slide 1

- Let me prepare you to a provoking presentation.
- Therefore, I will start off with a disclaimer: everything I say does neither represent my personal opinion nor that of the Netherlands. Everything I am about to say is based upon documentation I read when preparing this presentation. I merely deduced some conclusions out of this documentation, and asked myself some questions about it.
- By way of introduction to my presentation let me start with an overview of the Cyber Crime Convention and my understanding of it in relation to the topic of my presentation: cybercrime investigations and state sovereignty.
- The aim of the Cyber Crime Convention is, inter alia: to set up a fast and effective regime of international cooperation.
- The structure of the Convention is to provide for harmonised domestic substantive law; for harmonised domestic procedural law; to set up a system of international cooperation.
- In the Convention we tried to adapt the traditional procedural measures (e.g. search and seizure in a technical environment) and to create new measures such as expedited preservation (referring in general to and traffic and content and subscriber data).
- The jurisdiction issue in the Convention is based on the territoriality principle used in international law.
- At the same time the Convention introduces mutual legal assistance as an important asset in combating cybercrime; mutual legal assistance should be provided “in the widest extent possible”. And “assistance is to be extensive, impediments thereto to be limited”. Article 31 of the Convention states as much that State (party) searches and seizures are there for the benefit of another State.

##### Slide 2

- But my presentation is not about mutual legal assistance.
- Therefore a note on the field I am about to cover, the limitations to my presentation: I will talk about state sovereignty in as far as it relates to cross-border investigations in order to find evidence against a suspect. Although related to the question at hand, I will not dwell on jurisdiction, the territoriality principle or issues relating to mutual legal assistance.
- It's a controversial issue that was at the centre of debate at the time the Cyber Crime Convention was negotiated. Back then it was argued that there was a lack of experience and since the specific circumstances of the individual case are important, the text of article 32 of the Convention stands as it is. I will come to this later.
- But it is an ambiguous one too: is there really a problem in day to day practice? Or is it just a matter of national law and the limitations it puts on law enforcement services?

##### Slide 3

- The issues of sovereignty and jurisdiction are closely linked but not exchangeable. They are both, actually, quite separate entities.
- In short: sovereignty is determined by states, jurisdiction by law and legal practice.

- The two may collide when a state claims jurisdiction, investigates a case and – for this – needs to gain access data not available on its territory.
- No doubt you are aware of the situations I am talking about: you police forces gain knowledge of a cyber attack with links to computers (or data stored) in another state. You are in the position to get access – from your own territory – to those computers or data. Are you breaching the sovereignty of that other state?
- The France vs. Turkey Lotus case of 1927 determined that it would be a breach of sovereignty when law enforcement officials of a state conduct an investigation in another state without the other state's consent. Understandably for the era we are talking about, this judgment interpreted a state's sovereignty quite strictly. Nevertheless, it is still valid today when it comes to physical intrusions.
- The question here is: is there also a breach of sovereignty when the investigation activity on the other state's territory is not physical but only virtual? I will come to that in my next few sheets.
- Then there is article 32 b of the Cyber Crime Convention that states that: "A Party may, without the authorisation of another Party, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system."
- As I said before, at the time when the Convention was negotiated, it was considered that more experience was needed. For now transborder access to computer data is limited to situations where the "lawful owner" agrees to it or where information is publicly available. In 2000 it was considered that "other situations are not to be regulated until such time as further experience has been gathered. (...) [F]urther discussions may be held in light thereof. (...)" To further my quotes from the explanatory note attached to the Convention: "Other situations are neither authorised, nor precluded."
- Article 32 b is quite an interesting article for more than one reason: when should the authorisation be given, beforehand or is it okay if it comes after the search was completed? Another question: how on earth is it possible for an individual (the one with "lawful authority") to determine that a breach of sovereignty was committed or not? Because it is the person with lawful authority who holds the key to the door of state sovereignty? Was it considered, at the time that the Convention was drafted, to just add a sentence to article 32 b that says: "The sovereignty of states will be fully respected"?
- Finally, there is national law. I am not an expert in the legal texts of all the countries that ratified this Cyber Crime Convention but I assume that some countries define their sovereignty in their constitutions, others in specific laws. The interesting question here is how national law relates to article 32 b of the Cyber Crime Convention? How is access and reception defined in national law? What does lawful and voluntary consent mean in the national legal arena? Who is a person with lawful authority according to national law? What does authorisation really mean when it comes to a case in court? In other words: does article 32 b have a bearing on the national criminal code or is it just there for diplomatic reasons? The states that ratified the convention say that they will respect the sovereignty of any other state that ratified the convention?

#### Slide 4

- Let me continue my presentation by giving you some concrete examples that touch upon the sovereignty issue from three different angles. I'll bet the my examples are not unknown to you.

- First of all the Ivanov-Gorschkov case that evolved in the US. It became a *cause célèbre* in recent diplomatic history as it resulted in a diplomatic row between the US and the Russian Federation.
- Ivanov and Gorschkov are Russian nationals whom the FBI lured to the United States. They were arrested and charged with committing certain cyber crime offences. No doubt they were guilty, but that is not the issue here.
- The issue is that the FBI agents, in proving their case, downloaded evidence from Russian computers to assure that the information was not lost or destroyed by associates of the men in Russia. By the way, this was done before the agents were able to obtain a search warrant.
- Gorshkov challenged the case against him, arguing that the FBI had violated the Fourth Amendment of the U.S. Constitution, which protects against unreasonable search and seizures. He also argued that the search violated Russian law.
- I myself raised an eyebrow when reading that the U.S. court dealing with the case, judged that Gorshkov's Fourth Amendment rights were not violated, as it does not apply to extraterritorial searches against non-citizens. I know American law works that way. But it seems discriminatory to me just the same. But not even this is the most interesting part about this case for my argument.
- It rather is the opinion held by the U.S. Court that Russian law was not violated and, regardless, it was irrelevant to the matter in the United States. The literature I consulted about this case was as succinct about this part of the case as I am presenting to you know.
- I do not know what Russian law says about this particular case, but probably it will have something to do about legal rights of Russian citizens being breached when judged by a foreign court. Or it might say something about Russian sovereignty being breached.
- Of course I can understand the ruling that a US court is not bound by Russian law. But what I find most interesting is that the US court obviously didn't consider it in the least necessary to motivate its judgment that sovereignty rights were or weren't breached.
- The result was a diplomatic row, which may or may not have to do with the fact that it involved the US and the Russian Federation, two major powers in the world.
- Then my second example: the Australian law. Like in the Netherlands, under Australian federal law, search powers related to computer evidence are no longer confined to specific locations. The Cybercrime Act 2001 envisages that evidentiary data may be dispersed across a computer network, and allows searches for off-site data accessible through computers located on the search premises. However, it is also stipulated that notification is required, where practicable, of the occupier of the remote premises. Moreover, the Australian Telecommunications Interception Act does not authorise the interception by Australian authorities of telecommunications where the sender and the recipient are both overseas.
- Let me now come to the provision of Australian law that touches on my argument: the provision that it is prohibited for foreign governments to intercept telecommunications within Australia. I find this a clear example of a specific national law implicitly – or explicitly, depending on where you stand – stipulating where state sovereignty it touched upon.
- Finally, the Belgian law, our neighbouring country. For law enforcement purposes the provision of the 2000 Computer Crime Act are quite helpful. First the law stipulates that a computer search can – under certain circumstances - be expanded to an interconnected system situated in another place.
- The interesting part is that the order to a search can also be given, even if the data are not situated on Belgian territory. (And when data are found, only copying is allowed.)

What happens then is that the investigating judge shall report the extraterritorial search immediately to the Minister of Justice, who will subsequently inform the competent authority of the other state (Art. 88ter para. 3 CCP).

- I am not aware – at least I didn't do any in depth research into this – of the line of reasoning behind the phrasing of the Belgian law. But I can only assume that the Belgian legislature was of the opinion that a search into foreign computer systems – when started off in a Belgian system that is – counts for a non-physical intrusion. (The copy-only" provision would support this.) Informing the authorities of the other state – as a gesture of courtesy? – suffices.
- So, what we can see is that in the US – at least in the particular case I discussed – sovereignty of other states isn't a legal issue. The Australian example makes clear that states may define themselves where their sovereignty becomes an issue. Belgian law shows us that it is not all that clear whether a search on foreign computer, poses an intrusion to the sovereignty of other states.
- I can only imagine the legal and non-legal conflicts that may arise from all this.:-)

#### Slide 5

- I thought it would be just, to also say something about the law in my own country, the Netherlands.
- As far as I can see, Dutch law takes a traditionalist stance when it comes to the relation between computer searches and the sovereignty of other states.
- Our Cyber Crime Act dates back to the mid-1990s. We are in the process of updating it. But I do not foresee any substantial changes compared to the current situation.
- When it comes to searches articles 125 i, j and o of our Code of Penal Procedure are the most relevant articles. They were drafted to conform to the Cyber Crime Convention, and enacted in 2006. I will focus only on article 125j, most relevant to our debate. It states that in case of a search (in a house or office) it is warranted to search computers present on that location, when the warrant allows that much. Searches must be done on location. Network searches or continued searches are also allowed (within certain limits), in as far as it granted by the rightful owner. Otherwise the examining judge can order the passwords to be given (except to the suspect, who is not obliged to incriminate himself).
- For searches to continue on systems outside the Netherlands the explanatory note of our Cyber Crime Act stipulates that this is not allowed other than through international public law. In practical terms, law enforcement should resort to mutual legal assistance.
- The provisions of article 24 of the Intelligence Services Act are broader than those of the Code of Criminal Procedure, but not when it comes to systems located outside the Netherlands.
- The last bullet-point (legal protection, privacy and notification rules) speak for themselves. They are not necessarily part of the debate surrounding sovereignty. I just wanted to mention them here, as I consider them to be the necessary counterbalance for all search rights endowed to our law enforcement services.

#### Slide 6

- So, we come to the situation in 2010 as compared to the year 2000 when the drafting of the Cyber Crime Convention was finalised.
- New developments: from stand alone use to networked use, the rise of cloud computing, societies more dependent on ICT, changes in the way computer criminals work.
- As discussed when drafting the Convention: unilateral use of investigating powers/means is in principle permitted because of:
  - a) the need to act and get hold of probably volatile data;

- b) the absence of certainty of the whereabouts of the data in the world;
- c) States provide each other assistance to the “widest extend” possible.
- Of course I am best informed on investigations done in the Netherlands. Our law enforcement services have a lot more experience in doing online network searches and looking into web mail accounts like hotmail.
- But they also encounter new challenges, for example the use of the draft folder in web based e-mail accounts. Searching them proves to be very difficult and time consuming.

**Slide 7**

- There is a need for sharing best practices on what is possible.
- Maybe alter our domestic law on a number of fields.
- Re-drafting amendments to article 32 b.
- Greatest dangers: protection of rights of citizens, consumers, end users.
- Another precondition: fair investigation.