COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

www.coe.int/TCY

Strasbourg, 15 November 2016 T-CY (2016)32

Cybercrime Convention Committee (T-CY)

16th Plenary

Strasbourg, 14 – 15 November 2016

Meeting report

1 Introduction

The 16th Plenary of the T-CY Committee, meeting in Strasbourg on 14 and 15 November 2016, was chaired by Erick PLANKEN (Netherlands) and opened by Jan KLEIJSSEN (Director of Information Society and Action against Crime, DG 1, Council of Europe). Some 170 representatives of State Parties and Observers participated.

2 Decisions

The T-CY decided:

Agenda item 2: Status of signatures, ratifications, accessions to the Budapest Convention and its Protocol

- To take note of steps underway in view of ratification or accession to the Convention or its Protocol by Argentina, Austria, Chile, Colombia, Costa Rica, Ghana, Mexico, Monaco, Morocco, Philippines, Senegal, South Africa and Tonga;

- To welcome the interest in the Budapest Convention by the ad-hoc Observers of Belarus, Cabo Verde, Korea, Singapore and Tunisia;

- To encourage States that have signed or been invited to accede to become Parties as soon as possible;

- To request the T-CY Bureau and Secretariat to undertake T-CY visits to States that have signed or been invited to accede to the Convention to facilitate completion of the process;

- To invite T-CY members to support the accession process, including in consultation with their respective Representations in Strasbourg, in line with the T-CY work-plan;

- To remind States that instruments of accession or ratification must include declarations on competent authorities for extradition (Article 24 Budapest Convention) and mutual legal assistance (Article 27) as well as the 24/7 point of contact (Article 35);

- To encourage all States that are Parties to the Budapest Convention to sign, ratify or accede to the Additional Protocol (ETS 189) on Xenophobia and Racism committed through computer systems;

- To underline the global value and relevance of the Budapest Convention as expressed by T-CY participants from all continents;

Agenda item 3: Information provided by Parties and Observers – Tour de table

- To note with interest information provided on cybercrime policies, legislative developments, training or major cases by Albania, Argentina, Armenia, Australia, Austria, Azerbaijan, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Cabo Verde, Chile, Colombia, Costa Rica, Croatia, Czech Republic, Denmark, Dominican Republic, Estonia, Finland, France, Georgia, Germany, Ghana, Hungary, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Liechtenstein, Mauritius, Mexico, Moldova, Montenegro, Monaco, Morocco, Netherlands, Norway, Philippines, Poland, Portugal, Romania, Russian Federation, Senegal, Serbia, Singapore, Slovakia, Slovenia, Spain, Sri Lanka, South Africa, Switzerland, “The former Yugoslav Republic of Macedonia”, Tonga, Tunisia, Turkey, Ukraine and USA;

Agenda item 4: Dialogue with international organisations (T-CY observers)

- To welcome the information provided by the European Union (European Commission, EUROJUST and ENISA), Commonwealth Secretariat, INTERPOL, the Organisation of American States (OAS) and the Organisation for Security and Co-operation in Europe (OSCE);

Agenda item 5: Cloud Evidence Group: Consideration of draft outcome

- To welcome with appreciation the report of the Cloud Evidence Group and with regard to:

  - Recommendation 1, the T-CY agrees that Parties should give follow up to the T-CY Recommendations on MLA adopted in December 2014 and falling primarily under the responsibility of domestic authorities, that is, Recommendations 1 to 15.[1] The T-CY to review progress made, and capacity building programmes, if necessary, to support implementation;

  - Recommendation 2, the T-CY notes broad support to the draft Guidance Note on Production Orders for Subscriber Information as revised during the 16th Plenary but that some Parties require further consultation within their capitals. It invites Parties to provide written comments, if any, on the draft Guidance Note (version 15 November 2016) by 10 December 2016 to permit adoption or further consultations. In case of need for further consultations, interested Parties are invited to a meeting with the Cloud Evidence Group on 30-31 January 2017. Comments and observations by Observer States and Organisations are welcome at any time;

  - Recommendation 3, the T-CY agrees to invite Parties and Observer States to review domestic procedures for access to subscriber information and thus to ensure full implementation of Article 18 Budapest Convention;

  - Recommendation 4, the T-CY agrees to pursue practical measures – pending longer-term solutions – to facilitate more coherent cooperation between service providers and criminal justice authorities, including:

    - for the T-CY to hold annual meetings with providers;
    - the T-CY Secretariat and the C-PROC to maintain an online resource on provider policies and procedural rules in Parties;
    - C-PROC to involve providers in capacity building projects;
    - the T-CY to liaise with the EU Commission;

  - Recommendation 5, the T-CY agrees in principle on the need for an Additional Protocol. In order to facilitate a formal T-CY decision by June 2017 on initiating the drafting of a Protocol, the T-CY extends the mandate of the Cloud Evidence Group and requests the CEG to submit draft Terms of Reference for the drafting process and additional information on possible elements to the T-CY in spring 2017.

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

Agenda item 6: Status of 3rd round of T-CY assessments on Article 13 on sanctions and measures

- To take note of the status of the T-CY assessment report on Article 13 and of the approach proposed by the T-CY Bureau;

- To invite the Bureau to prepare and circulate a draft assessment report in May 2017 for consideration by the 17th Plenary of the T-CY in June 2017;

Agenda item 7: Follow up to Assessment Report on Mutual Legal Assistance

- To underline the importance of increasing the efficiency of mutual legal assistance on cybercrime and electronic evidence and thus of giving follow up to the T-CY Recommendations adopted in December 2014;

- To note with appreciation the support provided on follow up to the T-CY Recommendations on mutual legal assistance in countries of the Eastern Partnership region through the joint project of the European Union and the Council of Europe Cybercrime@EAP II;

- To welcome the replies to the questionnaire on follow up given by 18 Parties; and to invite the remaining Parties and Observer States to provide their replies no later than 15 December 2016;

- To invite the T-CY Bureau to submit a report on follow up given for consideration by the 17th Plenary of the T-CY in June 2017;

- To welcome the online tool on mutual legal assistance developed by the Council of Europe under the Octopus Community and to invite Parties to complete this tool with relevant information;

- To take note of the results of “ping tests” carried out by the T-CY Secretariat to verify the functioning of 24/7 points of contact, and to invite T-CY representatives to follow up at domestic levels to clarify responsibilities, contact details and procedures if necessary;

Agenda item 8: Guidance Notes

- To adopt the T-CY Guidance Note on Aspects of Terrorism covered by the Budapest Convention (T-CY (2016)11);

- To take note of the information provided by Ukraine on cyberattacks against critical infrastructure;

Agenda item 9: Financial resourcing of the T-CY for 2016/17

- To note with appreciation the voluntary contributions by Estonia, Japan, Monaco and USA to the Cybercrime@Octopus project for 2016/2017, including in view of support to the T-CY;

- To call on Parties and Observers to provide additional, preferably non-earmarked, contributions to the Cybercrime@Octopus project, including in view of support to the T-CY;

Agenda item 10: Activities of capacity building projects and the Cybercrime Programme Office of the Council of Europe (C-PROC)

- To note with appreciation the increasing scope of capacity building activities implemented through the Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania;

- To thank donors (Estonia, Japan, Monaco, Romania, United Kingdom and the USA) for voluntary contributions for capacity building, and the European Union for funding provided under joint projects of the Council of Europe and the European Union;

- To call on the Council of Europe,
  - to provide in particular Parties, Signatories and States invite to accede to the Budapest Convention with the full range of capacity building activities, including training, on the ground;
  - to support any State interested in the Budapest Convention in the strengthening of domestic legislation on cybercrime and electronic evidence;
  - to contribute to relevant activities of partner organisations;

Agenda item 11: Any other business

- To note strong support for the establishment a T-CY Working Group on cyber bullying and other forms of online violence, especially against women and children – based on Article 1.1.j of the T-CY Rules of Procedure – and

  - to task the Group to study the topic in the form of a mapping exercise, including comparative approaches to legislation as well as documentation of good practices in view of presenting interim results to the 17th Plenary and a final report to the 18th Plenary of the T-CY;
  - to appoint Markko KUNNAPU (Estonia), Erik PLANKEN (the Netherlands), Gareth SANSOM (Canada), Betty SHAVE (Consultant), Cristina SCHULMAN (Romania), Eirik Tronnes HANSEN (Norway), Lilija OMELJANCUK (Lithuania), Branislav KADLECIK (Slovakia);
  - to welcome that other Parties are prepared to provide written contributions;
  - to hold meetings in conjunction with meetings of the T-CY Bureau, without defrayal of expenses other than cost foreseen for the Bureau, unless voluntary contributions become available;

Agenda item 12: Next meeting of the T-CY

To hold the 17th Plenary of the T-CY in Strasbourg in the period 19 to 21 June 2017[2], subject to funding.

[2] The dates of the 17th Plenary have been changed to 07-09 June 2017.

3 Appendix

3.1 Annotated agenda

(Please note that agenda items marked with * are for decision by the members representing contracting Parties to the Budapest Convention)

1. Opening of the 16th Plenary and adoption of the agenda
2. Status of signatures, ratifications, accessions to the Budapest Convention and its Protocol Participants are invited to discuss the status of signature, ratification or accession by specific countries.
3. Information provided by parties and observers – Tour de table Participants are invited to present information on legislative developments, major cases, important events, training provided to other countries, including by international organisations etc. Signatories and States invited to accede are invited to report on progress made towards ratification/accession to the Budapest Convention on Cybercrime and its Protocol on Xenophobia and Racism. Brief interventions (2 minutes per intervention).
4. Dialogue with international organisations (T-CY observers) Representatives of international organisations with observer status in the T-CY are invited to present relevant activities and engage in a dialogue with T-CY members. Observers include the African Union Commission, Commonwealth Secretariat, European Union (Commission, ENISA, EUROJUST, EUROPOL), INTERPOL, ITU, OAS, OECD, OSCE, UNODC, and G7.
5. Cloud Evidence Group: Consideration of draft outcome The T-CY is invited to consider: - The final Report of the Cloud Evidence Group; - The draft Guidance Note on the production of subscriber information (Article 18 Budapest Convention) in view of adoption; - Recommendations proposed by the Cloud Evidence Group in its Final Report in view of adoption; - Follow-up to be given by the T-CY.
6. Status of 3rd round of T-CY assessments on Article 13 on sanctions and measures T-CY 11 decided to dedicate the 3rd cycle of assessments on Article 13 (sanctions and measures) and adopted the questionnaire. The T-CY Bureau will update the Plenary on the current status of the assessment report.
7. Follow up to Assessment Report on Mutual Legal Assistance The T-CY assessment report on mutual legal assistance invites Parties to follow up on recommendations falling under the responsibility of domestic authorities and to report back to the

T-CY no later than 18 months from adoption of this report on measures taken to permit the T-CY, in line with the Rules of Procedure (Article 2.1.g), to review progress made.

The Secretariat will report on replies received from Parties to a questionnaire on follow up given to the Recommendations on MLA.

The Secretariat will present the online tool on international cooperation.

8. Guidance Notes

The T-CY is invited to consider:

- Draft Guidance Note on Terrorism in view of adoption;

- Case study on attacks against power plants in Ukraine.

9. Financial resourcing of the T-CY for 2016/17

The Secretariat will inform participants on the state of financial resources available for the T-CY in 2016 and 2017.

Following the decision on T-CY financing taken at the 9th Plenary, Parties are invited to consider financial support to the T-CY through voluntary contribution to the CYBERCRIME@OCTOPUS project.

10. Activities of capacity building projects and the Cybercrime Programme Office of the Council of Europe (C-PROC)

The Secretariat will provide an update of capacity building projects and the Council of Europe Programme Office on Cybercrime (C-PROC) in Bucharest.

11. Any other business

- T-CY working group on cyber bullying and other forms of online violence against women and children
  The Bureau proposes to establish a working group – based on Article 1.1.j of the T-CY Rules of Procedure - to study the topic in the form of a mapping exercise, including comparative approaches to legislation as well as documentation of good practices. A more focused study could follow afterwards. The working group would meet in conjunction with the next Bureau meeting. Interim results of the mapping exercise could be presented to the T-CY in June 2017. Markko KUNNAPU (Estonia), Eirik PLANKEN (the Netherlands), Gareth SANSOM (Canada), Betty SHAVE (Consultant), Cristina SCHULMAN (Romania) and Eirik Tronnes HANSEN (Norway) volunteered for this group.

12. Next meeting of the T-CY*

T-CY members are invited to decide on the proposal to hold T-CY 17 in June 2017.

This proposal is subject to the availability of funding.

3.2 Draft Guidance Note on the Production of Subscriber information (as revised during the 16th Plenary)

www.coe.int/TCY

Strasbourg, version 15 November 2016 T-CY(2015)16

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #10 (DRAFT)

Production orders for subscriber information

(Article 18 Budapest Convention)

Revised version as discussed by the T-CY at its 16th Plenary (14-15 November 2016)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[3]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note[4] addresses the question of production orders for subscriber information under Article 18, that is, situations in which:

- a person ordered to produce specified computer data is present in the territory of a Party (Article 18.1.a);[5]
- a service provider ordered to produce subscriber information is offering a service in the territory of the Party without necessarily being located in the territory (Article 18.1.b).

A Guidance Note on these aspects of Article 18 is relevant given that:

- subscriber information is the most often sought data in criminal investigations;
- Article 18 is a domestic power;
- the growth of cloud computing and remote data storage has raised a number of challenges for competent authorities seeking access to specified computer data – and, in particular, subscriber information – to further criminal investigations and prosecutions;
- currently, practices and procedures, as well as conditions and safeguards for access to subscriber information vary considerably among Parties to the Convention;
- concerns regarding privacy and the protection of personal data, the legal basis for jurisdiction pertaining to services offered in the territory of a Party without the service provider being established in that territory, as well as access to data stored in foreign jurisdictions or in unknown or multiple locations "within the cloud" need to be addressed;
- the enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note and that some Parties may request subscriber information through mutual legal assistance.

Article 18 is a measure to be applied in specific criminal investigations and proceedings within the scope of Article 14 Budapest Convention. Orders are thus to be served in specific cases with regard to specified subscribers.

[3] See the mandate of the T-CY (Article 46 Budapest Convention).
[4] This Guidance Note is based on the work of the T-CY Cloud Evidence Group.
[5] It is important to recall that Article 18.1.a of the Budapest Convention is not limited to subscriber information but concerns any type of specified computer data. This Guidance Note, however, addresses the production of subscriber information only.

2 Article 18 Budapest Convention[6]

2.1 Text of the provision

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

Extract from the Explanatory Report:

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.[7]

The requirement that the subscriber information to be produced is relating to services of a provider offered in the territory of the Party is considered to be met even if those services are provided via a technical geographic domain referring to another jurisdiction.

[6] See Appendix for Article 18 and extracts from the Explanatory Report in full.
[7] Paragraph 173 Explanatory Report.

2.2 What is "subscriber information?"

The term "subscriber information" is defined in Article 18.3 of the Budapest Convention:

> 3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
>
> a the type of communication service used, the technical provisions taken thereto and the period of service;
>
> b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
>
> c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Obtaining subscriber information represents a lesser interference with the rights of individuals than obtaining traffic data or content data.

2.3 What is a "service provider?"

The Budapest Convention on Cybercrime applies a broad concept of "service provider" which is defined in Article 1.c of the Budapest Convention:

For the purposes of this Convention:

> c "service provider" means:
>
> i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
>
> ii any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Article 18.1.b is to be applied with respect to any service provider present in the territory or offering a service in the territory of the Party.[8]

3 T-CY interpretation of Article 18 Budapest Convention with respect to subscriber information

3.1 The scope of Article 18.1.a

- The scope is broad: a "person" (which may include a "service provider") that is present in the Party's territory.
- With respect to computer data, the scope is broad but not indiscriminate: any "specified" computer data [2](hence Article 18.1.a is not restricted to "subscriber information" and covers all types of computer data).
- The specified computer data is in that person's possession or control.
- The specified computer data is stored in a computer system or a computer-data storage medium.
- The production order is issued and enforceable by the competent authorities in the Party in which the order is sought/granted.

[8] European Union instruments distinguish between providers of electronic communication services and of Internet society services. The concept of "service provider" of Article 1.c Budapest Convention encompasses both.

3.2 The scope of Article 18.1.b

The scope of Article 18.1.b is narrower than that of Article 18.1.a. Subsection b:

- is restricted to a "service provider;"[9]
- is restricted to "subscriber information;"
- the service provider which is served the order is not necessarily physically present, but the service is offered in the territory.

3.3 Jurisdiction

Article 18.1.b is restricted to circumstances in which the criminal justice authority issuing the production order has jurisdiction over the offence in line with Article 22 Budapest Convention.[10]

This may typically include situations in which the subscriber is or was resident or present on that territory when the crime was committed.

The present interpretation of Article 18 is without prejudice to broader or additional powers under the domestic law of Parties.

Agreement to this Guidance Note does not entail consent to the extraterritorial enforcement of a domestic production order issued by another State or create new obligations or relationships between the Parties.

3.4 What are the characteristics of a "production order?"

A "production order" under Article 18 is a domestic measure and is to be provided for under domestic criminal law. A "production order" is constrained by the adjudicative and enforcement jurisdiction of the Party in which the order is granted.

Production orders under Article 18 "refer to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services".[11]

---

[9] The "person" is a broader concept than "a service provider", although a "service provider" can be "a person".

[10] Article 22 – Jurisdiction

1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:
   a in its territory; or
   b on board a ship flying the flag of that Party; or
   c on board an aircraft registered under the laws of that Party; or
   d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.

3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.

4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.

5 When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

[11] Paragraph 172 Explanatory Report.

The Explanatory Report (paragraph 171) to the Budapest Convention refers to production orders as a flexible measure which is less intrusive than search or seizure or other coercive powers and which may serve as an appropriate legal basis for cooperation with service providers.

3.5 What effect does the location of the data have?

The storage of subscriber information in another jurisdiction does not prevent the application of Article 18 Budapest Convention. The Explanatory Report, states with respect to:

- Article 18.1.a that "the term 'possession or control' refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory."[12]

- Article 18.1.b that "the term 'possession or control' refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company)."[13]

This includes situations in which the storage facility is located outside of its territory.

Regarding Article 18.1.b, a typical situation may include a service provider that has its headquarters in one jurisdiction, applies the legal regime of a second jurisdiction, and stores the data in a third jurisdiction. Data may be mirrored in several jurisdictions or move between jurisdictions according to service provider discretion and without the knowledge or control of the subscriber. Legal regimes increasingly recognize, both in the criminal justice sphere and in the privacy and data protection sphere, that the location of the data is not the determining factor for establishing jurisdiction.

3.6 What is "offering a service in the territory of a Party?"

The growth of cloud computing has raised questions as to when a service provider is considered to be offering its services in the territory of the Party and thus may be issued a domestic production order for subscriber information. This has led to a range of interpretations across multiple jurisdictions by courts in both civil and criminal cases.

The T-CY has determined that with regard to Article 18.1.b, a service provider is "offering a service in the territory of the Party", when:

- the service provider enables persons in the territory of the Party to subscribe to its services (and does not, for example, block access to such services);

and

- orients its activities toward such subscribers (for example, by providing local advertising or advertising in the language of the territory of the Party), or makes use of the subscriber information (or associated traffic data) in the course of its activities, or interacts with subscribers in the Party.

A Party may require that for the purposes of a domestic production order the service be offered in a manner so that the provider may be considered to be established in the territory, or to have otherwise a real and substantial connection to the territory of the Party.

[12] Paragraph 173 Explanatory Report. A "person" in Article 18.1.a Budapest Convention may be a physical or legal person, including a service provider.
[13] Paragraph 173 Explanatory Report.

3.7 General considerations and safeguards

It is presumed that the Parties to the Convention form a community of trust and that rule of law and human rights principles are respected in line with Article 15 Budapest Convention.

> Article 15.3 - To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.

3.8 Applying Article 18 with respect to subscriber information

The production of subscriber information under Article 18 Budapest Convention may, therefore, be ordered if the following criteria are met in a specific criminal investigation and with regard to specified subscribers:

<table>
<tr><td colspan="3">IF
The criminal justice authority has jurisdiction over the offence in line with Article 22 Budapest Convention;</td></tr>
<tr><td colspan="3">AND IF
the service provider is in possession or control of the subscriber information;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td>Article 18.1.a
The person is in the territory of the Party. For example, the person is registered as a provider of electronic communication services, or servers or parts of its infrastructure are located in the Party.</td><td>OR</td><td>Article 18.1.b
The service provider is “offering a service in the territory of the Party”, when, for example:
- the service provider enables persons in the territory of the Party to subscribe to its services,[14] AND
- orients its activities at subscribers, or makes use of subscriber information in the course of its activities, or interacts with subscribers in the Party;</td></tr>
<tr><td colspan="3">AND IF</td></tr>
<tr><td></td><td></td><td>- the subscriber information to be produced is relating to services of a provider offered in the territory of the Party, even if those services are provided via a technical geographic domain referring to another jurisdiction</td></tr>
</table>

4 T-CY statement

The T-CY agrees that the above represents the common understanding of the Parties as to the scope and elements of Article 18 Budapest Convention with respect to the production of subscriber information.

[14] Note Paragraph 183 Explanatory Report: “The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider’s services.”

5 Appendix: Extracts of the Budapest Convention

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service provider's possession or control.

2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:

a the type of communication service used, the technical provisions taken thereto and the period of service;

b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.

Explanatory Report

Production order (Article 18)

170. Paragraph 1 of this article calls for Parties to enable their competent authorities to compel a person in its territory to provide specified stored computer data, or a service provider offering its services in the territory of the Party to submit subscriber information. The data in question are stored or existing data, and do not include data that has not yet come into existence such as traffic data or content data related to future communications. Instead of requiring States to apply systematically coercive measures in relation to third parties, such as search and seizure of data, it is essential that States have within their domestic law alternative investigative powers that provide a less intrusive means of obtaining information relevant to criminal investigations.

171. A "production order" provides a flexible measure which law enforcement can apply in many cases, especially instead of measures that are more intrusive or more onerous. The implementation of such a procedural mechanism will also be beneficial to third party custodians of data, such as ISPs, who are often prepared to assist law enforcement authorities on a voluntary basis by providing data under their control, but who prefer an appropriate legal basis for such assistance, relieving them of any contractual or non-contractual liability.

172. The production order refers to computer data or subscriber information that are in the possession or control of a person or a service provider. The measure is applicable only to the extent that the person

or service provider maintains such data or information. Some service providers, for example, do not keep records regarding the subscribers to their services.

173. Under paragraph 1(a), a Party shall ensure that its competent law enforcement authorities have the power to order a person in its territory to submit specified computer data stored in a computer system, or data storage medium that is in that person's possession or control. The term "possession or control" refers to physical possession of the data concerned in the ordering Party's territory, and situations in which the data to be produced is outside of the person's physical possession but the person can nonetheless freely control production of the data from within the ordering Party's territory (for example, subject to applicable privileges, a person who is served with a production order for information stored in his or her account by means of a remote online storage service, must produce such information). At the same time, a mere technical ability to access remotely stored data (e.g. the ability of a user to access through a network link remotely stored data not within his or her legitimate control) does not necessarily constitute "control" within the meaning of this provision. In some States, the concept denominated under law as "possession" covers physical and constructive possession with sufficient breadth to meet this "possession or control" requirement.

Under paragraph 1(b), a Party shall also provide for the power to order a service provider offering services in its territory to "submit subscriber information in the service provider's possession or control". As in paragraph 1(a), the term "possession or control" refers to subscriber information in the service provider's physical possession and to remotely stored subscriber information under the service provider's control (for example at a remote data storage facility provided by another company). The term "relating to such service" means that the power is to be available for the purpose of obtaining subscriber information relating to services offered in the ordering Party's territory.

174. The conditions and safeguards referred to in paragraph 2 of the article, depending on the domestic law of each Party, may exclude privileged data or information. A Party may wish to prescribe different terms, different competent authorities and different safeguards concerning the submission of particular types of computer data or subscriber information held by particular categories of persons or service providers. For example, with respect to some types of data, such as publicly available subscriber information, a Party might permit law enforcement agents to issue such an order where in other situations a court order could be required. On the other hand, in some situations a Party might require, or be mandated by human rights safeguards to require that a production order be issued only by judicial authorities in order to be able to obtain certain types of data. Parties may wish to limit the disclosure of this data for law enforcement purposes to situations where a production order to disclose such information has been issued by judicial authorities. The proportionality principle also provides some flexibility in relation to the application of the measure, for instance in many States in order to exclude its application in minor cases.

175. A further consideration for Parties is the possible inclusion of measures concerning confidentiality. The provision does not contain a specific reference to confidentiality, in order to maintain the parallel with the non-electronic world where confidentiality is not imposed in general regarding production orders. However, in the electronic, particularly on-line, world a production order can sometimes be employed as a preliminary measure in the investigation, preceding further measures such as search and seizure or real-time interception of other data. Confidentiality could be essential for the success of the investigation.

176. With respect to the modalities of production, Parties could establish obligations that the specified computer data or subscriber information must be produced in the manner specified in the order. This could include reference to a time period within which disclosure must be made, or to form, such as that the data or information be provided in "plain text", on-line or on a paper print-out or on a diskette.

177. "Subscriber information" is defined in paragraph 3. In principle, it refers to any information held by the administration of a service provider relating to a subscriber to its services. Subscriber information may be contained in the form of computer data or any other form, such as paper records. As subscriber information includes forms of data other than just computer data, a special provision has been included in the article to address this type of information. "Subscriber" is intended to include a broad range of

service provider clients, from persons holding paid subscriptions, to those paying on a per-use basis, to those receiving free services. It also includes information concerning persons entitled to use the subscriber's account.

178. In the course of a criminal investigation, subscriber information may be needed primarily in two specific situations. First, subscriber information is needed to identify which services and related technical measures have been used or are being used by a subscriber, such as the type of telephone service used (e.g., mobile), type of other associated services used (e.g., call forwarding, voice-mail, etc.), telephone number or other technical address (e.g., e-mail address). Second, when a technical address is known, subscriber information is needed in order to assist in establishing the identity of the person concerned. Other subscriber information, such as commercial information about billing and payment records of the subscriber may also be relevant to criminal investigations, especially where the crime under investigation involves computer fraud or other economic crimes.

179. Therefore, subscriber information includes various types of information about the use of a service and the user of that service. With respect to the use of the service, the term means any information, other than traffic or content data, by which can be established the type of communication service used, the technical provisions related thereto, and the period of time during which the person subscribed to the service. The term 'technical provisions' includes all measures taken to enable a subscriber to enjoy the communication service offered. Such provisions include the reservation of a technical number or address (telephone number, web site address or domain name, e-mail address, etc.), as well as the provision and registration of communication equipment used by the subscriber, such as telephone devices, call centers or LANs (local area networks).

180. Subscriber information is not limited to information directly related to the use of the communication service. It also means any information, other than traffic data or content data, by which can be established the user's identity, postal or geographic address, telephone and other access number, and billing and payment information, which is available on the basis of the service agreement or arrangement between the subscriber and the service provider. It also means any other information, other than traffic data or content data, concerning the site or location where the communication equipment is installed, which is available on the basis of the service agreement or arrangement. This latter information may only be relevant in practical terms where the equipment is not portable, but knowledge as to the portability or purported location of the equipment (on the basis of the information provided according to the service agreement or arrangement) can be instrumental to an investigation.

181. However, this article should not be understood as to impose an obligation on service providers to keep records of their subscribers, nor would it require service providers to ensure the correctness of such information. Thus, a service provider is not obliged to register identity information of users of so-called prepaid cards for mobile telephone services. Nor is it obliged to verify the identity of the subscribers or to resist the use of pseudonyms by users of its services.

182. As the powers and procedures in this Section are for the purpose of specific criminal investigations or proceedings (Article 14), production orders are to be used in individual cases concerning, usually, particular subscribers. For example, on the basis of the provision of a particular name mentioned in the production order, a particular associated telephone number or e-mail address may be requested. On the basis of a particular telephone number or e-mail address, the name and address of the subscriber concerned may be ordered. The provision does not authorise Parties to issue a legal order to disclose indiscriminate amounts of the service provider's subscriber information about groups of subscribers e.g. for the purpose of data-mining.

183. The reference to a "service agreement or arrangement" should be interpreted in a broad sense and includes any kind of relationship on the basis of which a client uses the provider's services. _____

5.2 Guidance Note on Aspects of Terrorism covered by the Budapest Convention (as adopted by the T-CY)

www.coe.int/TCY

Strasbourg, 15 November 2016 T-CY(2016)11

Cybercrime Convention Committee (T-CY)

T-CY Guidance Note #11

Aspects of Terrorism

covered by the Budapest Convention

Adopted by the 16th Plenary of the T-CY (14-15 November 2016)

Contact

Alexander Seger
Executive Secretary Cybercrime Convention Committee
Directorate General of Human Rights and Rule of Law
Council of Europe, Strasbourg, France

Tel +33-3-9021-4506
Fax +33-3-9021-5650
Email alexander.seger@coe.int

1 Introduction

The Cybercrime Convention Committee (T-CY) at its 8th Plenary (December 2012) decided to issue Guidance Notes aimed at facilitating the effective use and implementation of the Budapest Convention on Cybercrime, also in the light of legal, policy and technological developments.[15]

Guidance Notes represent the common understanding of the Parties to this treaty regarding the use of the Convention.

The present Note addresses how different Articles of the Convention could apply to terrorism.

Many countries are Parties to numerous treaties, and subject to UN Security Council Resolutions, that require criminalization of different forms of terrorism, facilitation of terrorism, support for terrorism, and preparatory acts. In terrorism cases, countries often rely on offenses that derive from those topic-specific treaties, as well as additional offenses in national legislation.

The Budapest Convention is not a treaty that is focused specifically on terrorism. However, the substantive crimes in the Convention may be carried out as acts of terrorism, to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

In addition, the procedural and international mutual legal assistance tools in the Convention are available to terrorism and terrorism-related investigations and prosecutions.

The scope and limits are defined by Articles 14.2 and 25.1 Budapest Convention:

> Article 14.2
> 2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:
> a the criminal offences established in accordance with Articles 2 through 11 of this Convention;
> b other criminal offences committed by means of a computer system; and
> c the collection of evidence in electronic form of a criminal offence.
>
> Article 25.1
> "The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence."

See also Articles 23 and 27.1 Budapest Convention as well as other Guidance Notes, such as the Guidance Notes on critical infrastructure attacks or distributed denial of service attacks.

[15] See the mandate of the T-CY (Article 46 Budapest Convention).

2 Relevant provisions of the Budapest Convention on Cybercrime (ETS 185)

2.1 Procedural provisions

The Convention's procedural powers (Articles 14-21) may be used in a specific criminal investigation or proceeding in any type of case, as Article 14 provides.

In fact, the specific procedural measures can be very useful, for example in terrorism cases, if a computer system was used to commit or facilitate the offence or if the evidence of that offence is stored in electronic form or if a suspect can be identified through subscriber information, including an Internet Protocol address. Thus, in terrorism cases, Parties may use expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools to collect electronic evidence in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

2.2 International mutual legal assistance provisions

The Convention's international cooperation powers (Articles 23-35) are of similar breadth.

Thus, Parties must make available expedited preservation of stored computer data, production orders, search and seizure of stored computer data, and other tools, as well as other international cooperation provisions, in order to cooperate with other Parties in terrorism and terrorism-related investigations and prosecutions within the scope set out above.

2.3 Substantive criminal law provisions

Finally, as noted above, terrorists and terrorist groups may carry out acts criminalized by the Convention as part of achieving their goals.

Relevant Articles	Examples
Article 2 – Illegal access	A computer system may be illegally accessed to obtain personally identifiable information (e.g. information about government employees to target them for attack).
Article 3 – Illegal interception	Non-public transmissions of computer data to, from, or within a computer system may be illegally intercepted to obtain information about a person's location (e.g. to target that person).
Article 4 – Data interference	Computer data may be damaged, deleted, deteriorated, altered, or suppressed (e.g. a hospital's medical records can be altered to be dangerously incorrect, or interference with an air traffic control system can affect flight safety).
Article 5 – System interference	The functioning of a computer system may be hindered for terrorist purposes (e.g. hindering the system that stores stock exchange records can make them inaccurate, or hindering the functioning of critical infrastructure).
Article 6 – Misuse of devices	The sale, procurement for use, import, distribution or other acts making available of computer passwords, access codes, or similar data by which computer systems may be accessed may facilitate a terrorist attack (e.g. it can lead to damage to a country's electrical power grid).
Article 7 – Computer-related forgery	Computer data (for example the data used in electronic passports) may be input, altered, deleted, or suppressed with the result that inauthentic data is considered or acted upon for legal purposes as if it were authentic.
Article 8 – Computer-related fraud	Computer data may be input, altered, deleted, or suppressed, and/or the function of a computer system may be interfered with, causing other persons

	to lose property (for example, an attack on a country's banking system can cause loss of property to a number of victims).
Article 11 – Attempt, aiding and abetting	Crimes specified in the treaty may be attempted, aided or abetted in furtherance of terrorism.
Article 12 – Corporate liability	Crimes covered by Articles 2-11 of the Convention in furtherance of terrorism may be carried out by legal persons who would be liable under Article 12.
Article 13 – Sanctions	Crimes covered by the Convention may pose a threat to individuals and to society, especially when the crimes are directed against systems that are crucial to daily life, for example public transport, banking systems or hospital infrastructure. The effects may differ in different countries, depending also on their degree of interconnectedness and their dependence on such systems. A Party may provide in its domestic law a sanction that is unsuitably lenient for terrorism-related acts in relation to Articles 2 - 11, and it may not permit the consideration of aggravated circumstances or of attempt, aiding or abetting. This may mean that Parties need to consider amendments to their domestic law. Parties should ensure, pursuant to Article 13 that criminal offences related to such acts "are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty". Parties may also consider aggravating circumstances, for example if such acts affect a significant number of systems or cause considerable damage, including deaths or physical injuries, or damage to critical infrastructure.

Other crimes covered by the Convention but not mentioned specifically above, including the production of child exploitation materials or trafficking in stolen intellectual property, may also be carried out in connection with terrorism.

For Parties to the Budapest Convention which are also Parties to the Additional Protocol on Xenophobia and Racism Committed Through Computer Systems (ETS 189)[16], two articles of the Protocol are relevant as these may relate to radicalisation and violent extremism which may lead to terrorism. These are Article 4 of the Protocol covering racist and xenophobic motivated threat and Article 6 covering denial, gross minimisation, approval or justification of genocide or crimes against humanity.

3 T-CY statement

The T-CY agrees that the substantive crimes in the Convention may also be acts of terrorism as defined in applicable law.

The substantive crimes in the Convention may be carried out to facilitate terrorism, to support terrorism, including financially, or as preparatory acts.

The procedural and mutual legal assistance tools in the Convention may be used to investigate terrorism, its facilitation, support for it, or preparatory acts.

[16] http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189

3.2 List of participants

1. Bureau members

Version 15 November 2016

COUNTRY	NAME	INSTITUTION
NETHERLANDS (T-CY Chair)	Erik PLANKEN Cloud Evidence Group member (T-CY Representative)	Senior Policy Advisor Cybercrime Law Enforcement Department Ministry of Justice
ROMANIA (T-CY Vice-chair)	Cristina SCHULMAN Cloud Evidence Group member (T-CY Representative)	Legal adviser Department for International Law and Judicial Cooperation Ministry of Justice
CANADA	Gareth SANSOM Cloud Evidence Group member (T-CY Representative)	Director, Technology and Analysis, Criminal Law Policy Section, Department of Justice Canada
DOMINICAN REPUBLIC	Claudio PEGUERO Cloud Evidence Group member (T-CY Representative)	Advisor to the chief of Police in ICT National Police
ESTONIA	Markko KÜNNAPU Cloud Evidence Group member (T-CY Representative)	Adviser on EU Affairs Ministry of Justice
MAURITIUS	Karuna Devi GUNESH-BALAGHEE Cloud Evidence Group member (T-CY Representative)	Assistant Solicitor General
NORWAY	Mr Eirik TRØNNES HANSEN Cloud Evidence Group member (T-CY Delegate)	Prosecutor Kripos
PORTUGAL	Pedro VERDELHO Cloud Evidence Group member (T-CY Representative)	Public Prosecutor General Prosecutor's Office of Lisbon Procuradoria Geral da Republica
SRI LANKA	Jayantha FERNANDO Cloud Evidence Group member (T-CY Representative)	Director ICTA
SWITZERLAND	Andrea CANDRIAN Cloud Evidence Group member (T-CY Representative)	Stv. Chef, International Criminal Law Unit Federal Office of Justice

COUNTRY	NAME	INSTITUTION
UKRAINE	Oleksii TKACHENKO Cloud Evidence Group member (T-CY Representative)	International Relations officer Cyber Department, SBU

2. Parties

COUNTRY	NAME	INSTITUTION
ALBANIA	Bledar DERVISHAJ (T-CY Representative)	Legal adviser Ministry of Justice
ALBANIA	Lysien ALI (T-CY Delegate)	Senior Expert IT Department Ministry of Justice
ALBANIA	Hergis JICA	Commissioner, Cybercrime Unit Albanian State Police
ALBANIA	Arqilea KOÇA	Prosecutor (chef of the sector) Cybercrime Sector Task –Force Department General Prosecution Office of Albania
ALBANIA	Aida VEIZAJ	Head of sector for money laundering State police directory
ARMENIA	Armen ABRAHAMYAN (T-CY Delegate)	Officer Fight Against High-tech Crimes, General Department of Struggle Against Organized Crime
ARMENIA	Armenuhi HARUTYUNYAN	Head of Department Legal Mutual Assistance Ministry of Justice
AUSTRALIA	Susan WHITAKER	Principal Legal Officer Australian Attorney-General's Department
AUSTRIA	Andrea ROHNER (T-CY Representative)	Prosecutor at the Ministry of Justice
AZERBAIJAN	Javid HUMBATOV	Ministry of National Security
BELGIUM	Frederik DECRUYENAERE (T-CY Representative)	Attaché au Service des Infractions et Procédures Particulières Service Public Fédéral Justice
BELGIUM	Nathalie CLOOSEN	Office of European Criminal Law of the Ministry of Justice
BOSNIA AND HERZEGOVINA	Branka BANDUKA (T-CY Representative)	Expert Adviser for combating organized crime Sector for combating terrorism, organized crime, corruption, war crimes and misuse of narcotics
BOSNIA AND HERZEGOVINA	Nedžad DILBEROVIĆ	Adviser, Section NBC Interpol, Directorate for Coordination of Police Bodies of Bosnia and Herzegovina

COUNTRY	NAME	INSTITUTION
BOSNIA AND HERZEGOVINA	Nedžad ĆATIĆ	Head of the Department for the fight against cybercrime, Ministry of the Interior of the Federation of Bosnia and Herzegovina
BOSNIA AND HERZEGOVINA	Darko CULIBRK	Investigator in Hi-Tech Crime Department Ministry of Interior of Republic of Srpska
BULGARIA	Vasil PETKOV T-CY Delegate	Inspector Cybercrime, IPR and Gambling Section, General Directorate Combating Organized Crime Ministry of Interior
CANADA	Erin MCKEY	Senior Counsel International Assistance Group Department of Justice Government of Canada
CANADA	Gareth SANSOM T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Director Technology and Analysis Criminal Law Policy Section Department of Justice Canada
CANADA	Dominic ARPIN	Cybercrime Coordinator Crime and Terrorism Division (IDT) Global Affairs Canada Government of Canada
CANADA	Cyndy NELSON	Legal Officer Criminal, Security and Diplomatic Law Division (JLA) Global Affairs Canada
CROATIA	Ivan MIJATOVIĆ	High-tech Crime Department National Police
CYPRUS		
CZECH REPUBLIC	Lenka HABRNÁLOVÁ (T-CY Representative)	International Cooperation and EU Department Ministry of Justice
DENMARK	Selina ROSENMEIER	Head of Section Criminal Law Division The Ministry of Justice
DOMINICAN REPUBLIC	Claudio PEGUERO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Advisor to the chief of Police in ICT National Police

COUNTRY	NAME	INSTITUTION
DOMINICAN REPUBLIC	César MOLINE	Attorney in charge of Competition Defense Encargado Defensa de la Competencia Dominican Institute of Telecommunications (Instituto Dominicano de las Telecomunicaciones - INDOTEL)
DOMINICAN REPUBLIC	Miguel JAZMIN	Member of the National Parliament Chairman of the National Commission for ICT House of Representatives, National Congress
DOMINICAN REPUBLIC	Thelma ALVAREZ	Legal Advisor / DICAT National Police
ESTONIA	Markko KÜNNAPU T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Adviser on EU Affairs Ministry of Justice
FINLAND	Janne KANERVA (T-CY Representative)	Counsellor of Legislation Legislative Affairs Ministry of Justice
FINLAND	Karl LINDERBORG	Senior Detective Superintendent, Legal Advisor, Deputy Head of Cybercrime Center National Bureau of Investigation Criminal Investigation, Cybercrime Center
FINLAND	Tiina FERM	Councellor in Legislative Affairs Police Department Ministry of the Interior
FRANCE	Sylvain BRUN (T-CY Delegate)	Adjoint au chef de OCLCTIC (National Cybercrime Unit) Sous-direction de la lutte contre la cybercriminalité Direction centrale de la police judiciaire Direction générale de la police nationale Ministère de l'Intérieur
FRANCE	Raphaele BAIL	Judge DACG
GEORGIA	Giorgi TIELIDZE (T-CY Representative	Senior Adviser Department of Internal Security and Public Order
GEORGIA	Givi BAGDAVADZE	

COUNTRY	NAME	INSTITUTION
GERMANY	Stefan ZIMMERMANN	Staff Counsel Division for Criminal Law Suppression of Economic Crime, Computer Crime, Corruption-related Crime and Environmental Crime Federal Ministry of Justice and Consumer Protection
HUNGARY	Zsuzsa PETHŐ (T-CY Representative)	Department of European Cooperation Ministry of Interior
ICELAND	Sigurður Emil PÁLSSON (T-CY Delegate)	Senior Advisor Civil Protection, Cyber Security, Critical Infrastructures, Technical and Strategic Issues Department of Public Security Ministry of the Interior
ISRAEL	Haim WISMONSKY (T-CY Representative)	Director, Cybercrime Department Israeli State Attorney's Office
ISRAEL	Naomi Elimelech Shamra (T-CY delegate)	Treaties Department Deputy Director Ministry of Foreign Affaires
ITALY	Francesco CAJANI Cloud Evidence Group member (T-CY Representative)	Deputy Public Prosecutor High Tech Crime Unit Court of Law in Milan
ITALY	Gianluigi UMETELLI	Chief Inspector Italian National Police
JAPAN	Yuri HAYASHI Cloud Evidence Group member	International Safety and Security Cooperation Division Foreign Policy Bureau Ministry of Foreign Affairs
JAPAN	Mayumi TSUBOI	Attorney Criminal Affairs Bureau Ministry of Justice
JAPAN	Fumitake MASUKAWA	Superintendent, Cybersecurity Office National Police Agency of JAPAN
LATVIA	Aleksandra TUKISA (T-CY Delegate)	International Cooperation Bureau
LATVIA	Uldis ĶINIS	Vice Presidents of Constitutional court/ professor Constitutional court of Latvia

COUNTRY	NAME	INSTITUTION
LITHUANIA	Lilija OMELJANČUK (T-CY Representative)	Chief Investigator of the 1st Division of Cybercrime Investigation Board of the Lithuanian Criminal Police Bureau Vilnius
LIECHTENSTEIN	Dominic SPRENGER (T-CY Representative)	Office for Foreign Affairs
LUXEMBOURG	Catherine TRIERWEILER (T-CY Representative) APOLOGISED	Attachée d'administration au Ministère de la Justice à Luxembourg
MALTA		
MAURITIUS	Karuna Devi GUNESH-BALAGHEE Bureau and Cloud Evidence Group member (T-CY Representative)	Assistant Solicitor General
MAURITIUS	Mary Jane LAU YUK POON Cloud Evidence Group member	Assistant Solicitor General Attorney General's Office
MAURITIUS	Divi SEWPAL	State Counsel
MAURITIUS	Pravin HARRAH	Principal State Counsel Office of the Director of Public Prosecutions
MAURITIUS	Michael Clint Kervin Juanito PUDMAN	Police Officer Mauritius Police Force
MOLDOVA	Veaceslav SOLTAN (T-CY Representative)	Prosecutor Chief of Department on Information Technology and Cybercrime Investigation
MOLDOVA	Irina CUCIUC	
MONTENEGRO	Jakša BACKOVIĆ	Head of Unit for Anti-High Tech Crime in the Department for the fight against organised crime and corruption, Ministry of Interior - Police Directorate
MONTENEGRO	Ognjen MITROVIC (T-CY Representative)	Adviser Directorate for International Legal Cooperation and EU Integration Ministry of Justice
MONTENEGRO	Aleksandra RUBEŽIĆ	Independent advisor – coordinator of Analytics Department Administration for the Prevention of Money Laundering and Terrorism Financing of Montenegro

COUNTRY	NAME	INSTITUTION
NETHERLANDS	Erik PLANKEN T-CY Chair and Cloud Evidence Group member (T-CY Representative)	Senior Policy Advisor Cybercrime Law Enforcement Department
NETHERLANDS	MAAS E.M.	Ministry Security and Justice
NORWAY	Eirik TRØNNES HANSEN T-CY Bureau and Cloud Evidence Group member (T-CY Delegate)	Prosecutor Kripos
PANAMA		
POLAND	Michał ZALEWSKI	Wydział dw. z Cyberprzestępczością Biuro Służby Kryminalnej Komendy Głównej Policji
PORTUGAL	Pedro VERDELHO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Public Prosecutor General Prosecutor's Office of Lisbon Procuradoria Geral da Republica
ROMANIA	Ioana ALBANI Cloud Evidence Group member (T-CY Delegate)	Deputy Chief-Prosecutor Directorate for Investigating Organised Crime and Terrorism Prosecutor's Office attached to the High Court of Cassation and Justice
ROMANIA	Cristina SCHULMAN T-CY Vice-Chair and Cloud Evidence Group member (T-CY Representative)	Legal adviser Department for International Law and Judicial Cooperation Ministry of Justice
SERBIA	Branko STAMENKOVIC (T-CY Representative)	Special Prosecutor for High-Tech Crime of Serbia
SERBIA	Jovana MIHAILOVIC	Legal Specialist Ministry of Justice
SERBIA	Dragan JOVANOVIC	Deputy Head of Department Service for Combating Organized Crime Department for Cyber Crime
SERBIA	Vlatko BOZOVIC	Head of Department for Financial Investigation Ministry of Interior
SLOVAKIA	Branislav KADLECIK (T-CY Representative)	General State Counsellor Office of the Minister Human Rights Divisin Ministry of Justice
SLOVENIA	Tomaž JAKSE	Senior Criminal Police Inspector – Specialist Computer Investigation Centre

COUNTRY	NAME	INSTITUTION
SPAIN	Maria Elvira TEJADA DE LA FUENTE (T-CY Representative)	Head Cybercrime Prosecutor's Office
SPAIN	Angel SANCHEZ FRAILE	Spanish National Police High Tech Unit
SPAIN	Jose DURAN	Guardia Civil Criminal Police Branch Criminal Intelligence Unit – High Tech Crime Group
SRI LANKA	Jayantha FERNANDO Bureau and Cloud Evidence Group member (T-CY Representative)	Director ICTA
SRI LANKA	Dharshika KUMARI	Woman Assistance Superintendent of Police Criminal Investigation Department
SRI LANKA	Roshan Chandraguptha GALABADA LIYANAGE	Principal Information Security Engineer
SRI LANKA	Hon. E.A.G.R. AMARASEKARA	High Court Judge, Commercial High Court Colombo
SWITZERLAND	Andrea CANDRIAN T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	Stv. Chef, International Criminal Law Unit Federal Office of Justice
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Vladimir MILOSHESKI (T-CY Representative)	Public Prosecutor Basic Public Prosecutor's Office
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Aleksander RISTOVSKI	IT Officer Financial Police Department Ministry of Finance
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Maja JOVANOVA	Head of IT Unit Department for Financial Intelligence
"THE FORMER YUGOSLAV REPUBLIC OF MACEDONIA"	Marjan STOILKOVSKI	Head of the Sector for Computer Crime and Digital Forensics
TURKEY	Kürşad Başaran BASOGLU	Captain Cybercrime Prevention Division Cybercrime Department Turkish National Police
TURKEY	Ömer Artun AKTİMUR	Financial Intelligence Unit (FIU) Financial Crimes Investigation Board Ministry of Finance

COUNTRY	NAME	INSTITUTION
TURKEY	Tamer SOYSAL	Judge Department of Justice
TURKEY	Meral GÖKKAYA	Investigating Judge Ministry of Justice
UKRAINE	Oleksii TKACHENKO T-CY Bureau and Cloud Evidence Group member (T-CY Representative)	International Relations officer Cyber Department, SBU
UKRAINE	Tetiana SHORSTKA	Deputy Head of Department-Head of the Division on Mutual Legal Assistance in Criminal Matters Ministry of Justice
UNITED KINGDOM	Faiza TAYAB-JONES APOLOGISED	Cyber Crime, Fraud, Interventions & Partnerships Unit Strategic Centre for Organised Crime Office for Security and Counter Terrorism
USA	Albert C. REES JR.	Senior Counsel, International Programs Computer Crime & Intellectual Property Section United States Department of Justice

3. Observer States

COUNTRY	NAME	INSTITUTION
ANDORRA	Azahara CASCALES RUIZ APOLOGISED	Juge d'instruction
ARGENTINA	Marcos SALT (T-CY representative)	Prof. Criminal Law University of Buenos Aires Academic Director National Program on computer Related Crime Ministry of Justice
CHILE	Pablo CASTRO (T-CY Representative)	Subdirector para Seguridad Internacional Ministerio de Relaciones Exteriores Dirección de Seguridad Internacional y Humana
COLOMBIA	Angel JUANITA NAVARRO	Crime Prevention Division Department of Political Multilateral Affairs Ministry of Foreign Affairs
COSTA RICA	Adalid MEDRANO (T-CY Delegate)	Abogado & Consultor en Nuevas Tecnologías
GHANA	Yvonne ATAKORA OBUOBISA	Ag. Director of Public Prosecutions Division
GHANA	Kwabena ADU-BOAHEN	Office of the National Security Coordinator
GHANA	Margaret ABBA-DONKOR	Manager Engineering National Communications Authority
GREECE		
IRELAND		
MEXICO	Santiago OÑATE LABORDE	Observateur Permanent du Mexique auprès du Conseil de l'Europe
MEXICO	Diego Sandoval PIMENTEL	Adjoint à l'Observateur Permanent du Mexique auprès du Conseil de l'Europe
MONACO	Gabriel REVEL	Adjoint au Représentant Permanent Représentation Permanente de Monaco auprès du Conseil de l'Europe
MONACO	Jacques DOREMIEUX	Public Prosecutor (General) Justice Parquet Général

COUNTRY	NAME	INSTITUTION
MOROCCO	Layla EZZOUINE	Chef de Service de lutte contre la criminalité liée aux nouvelles technologies Direction générale de la Sûreté nationale
MOROCCO	Abdeljalil TAKI (T-CY representative)	Ministère de l'Intérieur DGST
MOROCCO	Mina JAMIL	Magistrat Ministère de la Justice et des Libertés
PARAGUAY	María Soledad MACHUCA APOLOGISED	Head of Cybercrime Unit Deputy Attorney General
PERU	Milagros CASTANON SEANE APOLOGISED	Ministra SDR Directora de la Direccion de Ciencia Y tecnología DAE
PHILIPPINES	Wendell BENDOVAL	Prosecutor National Prosecution Service Department of Justice
PHILIPPINES	Antonio KHO	Undersecretary / Deputy Minister Department of Justice
PHILIPPINES	Jed Sherwin UY T-CY Representative	Director Office of Cybercrime Department of Justice
RUSSIAN FEDERATION	Konstantin KOSORUKOV	First Secretary, Legal Department of the Ministry of Foreign Affairs of the Russian Federation
RUSSIAN FEDERATION	Yulia TOMILOVA	Third Secretary, Department of New Threats and Challenges of the Ministry of Foreign Affairs of the Russian Federation
RUSSIAN FEDERATION	Anton MARKOVSKIY	Deputy to the Permanent Representative of the Russian Federation to the Council of Europe
SAN MARINO		
SENEGAL	Papa Assane TOURE	Secrétaire général Adjoint du Gouvernement Primature du Sénégal
SENEGAL	Samba SALL	Magistrat Doyen des juges d'instruction au tribunal de grande instance hors classe de Dakar
SENEGAL	Issa DIACK	Commandant Section Recherches de la Gendarmerie nationale

COUNTRY	NAME	INSTITUTION
SOUTH AFRICA	Zoyisile MSHUNQANE (T-CY Representative)	State Security Agency
SOUTH AFRCA	Rhulani Luckson MIHLANGA	Third Secretary Permanent mission of South Africa in Austria
SWEDEN	Mikael KULLBERG APOLOGISED	Rättssakkunnig Åklagarenheten Justitiedepartementet
TONGA	Adi Talanaivini MAFI	Legal Officer Ministry of Justice
TONGA	Aminiasi KEFU (T-CY Representative)	Solicitor General Attorney General Office

4. Ad-hoc country observers

COUNTRY	NAME	INSTITUTION
BELARUS	Aleksandr SUSHKO	
BELARUS	Zmicier BRYLOU	
CABO VERDE	Franklin Afonso FURTADO	Deputy Public Prosecutor General Prosecutor's Office of Cabo Verde Procuradoria Geral da República Praia
KOREA	In Gi LEE	Investigator Cybercrime investigation FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office)
KOREA	Seong Su AN	Chief Prosecutor Deputy Chief of FSID FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office
KOREA	Gwi il KIM	Senior Investigator Cybercrime investigation FSID of SPO (Forensic Science Investigation Department of Supreme Prosecutor's Office)
KOREA	Do Wook SHIN	Prosecutor / International Criminal Affairs International Criminal Affairs Division of Ministry of Justice
SINGAPORE	Kannan GNANASIHAMANI	Senior State Counsel Deputy Public Prosecutor Senior Director Technology Crime Unit Financial & Technology Crime Division Attorney-General's Chambers
SINGAPORE	Suhas MALHOTRA	Attorney-General's Chambers
TUNISIA	Mohamed MESSAI	Conseiller à la Cour d'Appel de Tunis

5. Observer Organisations

ORGANISATION	NAME	POSITION
AFRICAN UNION COMMISSION (AUC)		
COMMONWEALTH	Emma THWAITE	Assistant Legal Officer, Rule of Law Division Commonwealth Secretariat
EUROPEAN COMMISSION HOME AFFAIRS	Tjabbe Bos	Policy Officer European Commission DG Migration and Home Affairs Unit D2 – Fight against organised crime
EUROPEAN COMMISSION	Barbara MENTRÉ	Legislative Officer
EUROPEAN UNION EUROPOL (EC3)	Gregory MOUNIER APOLOGISED	Head of Outreach and Support
EUROPEAN UNION ENISA	Silvia PORTESI	Research and Analysis Expert ENISA European Union Agency for Network and Information Security
EUROPEAN UNION EUROJUST		
EUROPEAN UNION EUROJUST	Daniela BURUIANA	Chair of the Task Force on cybercrime Eurojust National member for Romania
G7 Group's High-Tech Crime Subgroup		
INTERPOL	John BARRY	ICT Law Programme Manager Data Protection and Programmes
INTERPOL	Sabine BERGHS	Legal Officer
INTERPOL	Christophe DURAND	Head of Strategy and Outreach IGCI
International Telecommunication Union (ITU)		
ORGANIZATION OF AMERICAN STATES (OAS)	Belisario CONTRERAS	Cyber Security Program Manager Inter-American Committee against Terrorism
ORGANIZATION OF AMERICAN STATES (OAS)	Rodolfo ORJALES	President, Group of Experts on Cybercrime
OECD		
OSCE	Margaret LAZYAN	Politico/Military Senior Assistant OSCE Office in Yerevan
UNODC		

6. Council of Europe experts

ORGANISATION	NAME	POSITION
Consultant	Betty SHAVE	Consultant

7. Council of Europe Committees

COMMITTEES	NAME	POSITION
CDMSI (Steering Committee on Media and Information Society)		
CDPC (European Committee on Crime Problems)		
PC-OC		
T-PD		

8. Council of Europe Secretariat

Name	Details
Jan KLEIJSSEN	Director of Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Patrick PENNINCKX	Head of Media, Information Society, Data Protection and Cybercrime Department Information Society and Action against Crime Directorate, Directorate General Human Rights and Rule of Law
Alexander SEGER	Executive Secretary of the Cybercrime Convention Committee Head of Cybercrime Division Head of Cybercrime Programme Office (C-PROC) Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Alexandru FRUNZA	Programme Officer Data Protection and Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Pierluigi PERRI	Programme Officer Data Protection and Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Marie AGHA-WEVELSIEP	Programme Officer Cybercrime Division Information Society and Action against Crime Directorate Directorate General of Human Rights and Rule of Law
Ana ELEFTERESCU	Project Officer Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Sinziana HANGANU	Project assistant Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Valérie SCHAEFFER	Project Assistant Cybercrime Division Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law
Alexandra-Adina TRANDAFIR	Project assistant Cybercrime Programme Office (C-PROC) Bucharest Information Society and Action against Crime Directorate Directorate General Human Rights and Rule of Law

9. Interpreters

Julia TANNER
Christopher TYCZKA
Sylvie BOUX

Derrick WORSDALE
Sergio ALVAREZ
Hans MÜHLE