www.coe.int/TCY

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Second Meeting of the 24/7 points of contact (CP) under Budapest Convention on Cybercrime

Strasbourg, 11 July 2018

Draft Summary report

The Secretariat of the Cybercrime Convention Committee (T-CY) with the support of Cybercrime@Octopus, GLACY+, iPROCEEDS and Cybercrime@EAP 2018 projects organised Second meeting of the 24/7 Network of contact points under the Budapest Convention on Cybercrime in the morning of 11 July 2018 at the Council of Europe premises in Strasbourg, France. The meeting was a follow up to the first meeting of the points of contact, held on 26-27 September 2017 at EUROPOL, Hague, Netherlands.

34 participants from Albania, Armenia, Australia (also representing the United Kingdom), Austria, Azerbaijan, Bosnia and Herzegovina, Belarus, Chile, Costa Rica, Dominican Republic, France, Georgia, Ghana, Jordan, Latvia, Lebanon, Mauritius, Moldova, Montenegro, Netherlands, Nigeria, Philippines, Romania, Senegal, Serbia, Spain, Tonga, Tunisia, Ukraine and United States attended the meeting.

The workshop, as a follow-up to the first meeting of the 24/7 Network, provided an opportunity to delve deeper into more focused subjects of discussions, such as templates for requesting data, production orders for subscriber information related to dynamic IP addresses, and cooperation of 24/7 contact points with service providers in other jurisdictions. Participants were furthermore invited to exchange views on the proposed EU Regulation on production and preservation orders and recently adopted US CLOUD Act.

Similar to the previous meeting, it was also an opportunity for representatives of criminal justice authorities of countries seeking accession or having recently acceded to the Budapest Convention to learn more about the establishment, role and functioning of the 24/7 CP Network.

At the opening of the meeting, the context of 24/7 CP Network as complex channel of cooperation was underlined, to signify the importance of work done by the 24/7 points of contact. Particular note was taken of the recent legislative proposal by the European Commission on improving cooperation with international service providers, through new legislative instruments such as European Production Order and European Preservation Order. Increasing number of countries acceding to the Convention since the first meeting of the Network in

September 2017 was highlighted, with new ratifications also required increasing capacity building activities to support setup or better skills of the cooperation officers. Note was taken of establishment of second points of contact in some countries, at which point the participants of the meeting also introduced themselves.

The first session of the meeting was devoted to review of results from the first meeting of 24/7 contact points, held on 26-27 September 2017 in Hague, Netherlands, and follow-up given to its findings. The topics of role, organization and responsibilities of the 24/7 contact points; proactivity of the 24/7 contact points for providing technical advices/support to other countries; execution of preservation requests and facilitation of mutual legal assistance (MLA) requests; initial draft templates regarding the preservation of data and MLA request for subscriber information according to Articles 29 and 31 from the Budapest Convention; results of the survey regarding the functioning and responsibilities of the 24/7 contact points in relation to relevant aspects – were reported to the meeting. An extended view on strengths and negative practices of the 24/7 contact points network, as detailed in the report of the first meeting, was also provided. The session concluded with the review of recommendations for improvement in the functioning of the 24/7 CP Network, adopted by the first meeting in September 2017.

A discussion on several subjects related to the functioning of the network ensued, which focused on the following aspects:

- Use of uniform encryption for emails transmitted through the 24/7 CP network;
- Lack of secure communication channel in the framework of the Budapest Convention (compared to e.g. Europol);
- Email spoofing that can be also a concern for the network;
- Obstacles from data protection regime in some countries for exchange of data via official emails;
- Difficulties to use Transport Layer Security (TLS), security certificates and other standards for security in order to apply to different institutions, even in a country-specific context.

Next session of the meeting focused on the updated templates for preservation of data (Articles 29/30 of the Convention) and MLA requests for subscriber information (Article 31 requests). Differences between initially discussed and finalized templates, adopted by the T-CY on 9 July 2018 in its 19th Plenary Session, were presented and discussed, as the templates have been re-worked to accommodate all suggestions and comments made by various countries and institutions between the two meetings.

Short interventions from France, Georgia and Moldova supported the use of templates in practice. French template was developed on the basis of draft CoE template to create uniform practice and ensure that more details can be sent; Georgia reported no practical use of the templates, but noted also the use of standard data for communications with the US; and Moldova noted increase of information flow and speed through the practical use of the CoE templates. Romania also noted the use of template similar to CoE draft, especially for internal requests and for confidentiality and urgency sections, while also noting that any follow up MLA request would be directed to competent authorities for execution. Austria suggested further automation of the templates, perhaps with use of XML format. The issue was raised on behalf of the UK noting that existence of blank fields on the template may pose legal challenges from the perspective of defense. It was also noted that templates may help to address the request to the competent authorities by increasing clarity of the request.

A short reference on the practical aspects of the European Court of Human Rights case of Benedik vs. Slovenia was made followed by discussions in respect to the differences between

static and dynamic IPs for the purposes of production of data. Following brief introduction of main aspects of the case, most of the interventions noted no difference in treatment between the two, only Austria noting different treatment (court orders required only for obtaining subscriber information related to dynamic IPs).

The final session of the meeting looked into the issues of cooperation with multinational service providers (MSPs) in the context of 24/7 points of contact. Netherlands introduced the issue by noting jurisdictional challenges related to processing of data, even where data servers were present in its territory, and further issue of sale of data/services, lack of user data (e.g. payment details) and client disclosure obligations were noted as obstacles to cooperation.

France outlined several best practices that make cooperation with MSPs successful. First, having dedicated unit within cyber police; second, conducting informal meetings and signing cooperation protocols makes difference, especially with "Big Five" of the US providers who provide a lot of information, even through voluntary disclosure. Last but not least, an information platform for information on requests for all providers, to which all police officers can log in and find relevant data, is a very helpful tool. Further discussion on cooperation protocols revealed that these were templates worked out together with the US DOJ and represented more of an agreement on the common format, done on an initiative of the cybercrime unit.

Several countries expressed lack of positive experience on cooperation with MSPs. To remedy this, Israel noted that some problems can be overcome by establishing contact with regional policy managers of large foreign providers; also, requesting real-time information requires more information sharing as well on the part of the Government concerned; and requesting data from Israeli providers would best be served through point of contact relationships established in the judicial authorities. This view was also supported by Azerbaijan, whose representative mentioned a positive example of cooperation with Facebook gaining assistance after establishing contact with regional director, which helped to clarify format of the request, resulting in positive response.

Romania noted no specialized cooperation service for relations with foreign providers, but use of dedicated channels was highlighted, as well as use of dedicated law enforcement portals provided by big providers. Analysis of requests and writing of a guide for national authorities to be followed whenever addressing a request were also shared as best practice, especially in the context of voluntary disclosure.

Differences between the data were highlighted and thus different practices of cooperation. Due to voluntary nature of disclosure from the US-based providers, practical problems remain, thus leading to the EU proposal for EU Directive on production and preservation orders. There was limited discussion on the subject, which is addressed to the EU member states jurisdictions mostly.

Also the discussion on the recent US Cloud Act took place, which allows US authorities to obtain data in the possession and control of US providers regardless data is not located in the US soil and bilateral treaties to remove restrictions with access to data, effectively allowing foreign countries to serve their production orders on the US providers, albeit with no enforcement mechanism envisaged yet. Discussion revealed that in certain respects WHOIS holds the same data and ICANN search for temporary and long-term solution is equally important.

At this point, recent developments for establishing alternative points of contact in Armenia, Azerbaijan and Georgia as a result of capacity building efforts were briefly presented by the Cybercrime@EAP 2018 project.

The meeting closed with the topics for the agenda of the next meeting, and thus several proposals were identified:

- The subject of safe communications in wide sense (Netherlands);
- Assessment and feedback on the use of the templates together with MLA communications and coordination between MLA and 24/7 processes (Cybercrime@EAP 2018 project);
- Role and functioning of 24/7 contact points for further improvements in the cooperation and development of new instruments of the Network (Israel);
- Discussion on European preservation/production orders requiring judicial authorization-future perspective (Spain);
- Proposal for full one-day meeting for the entire 24/7 CP Network, separate from other events (C-PROC).

In conclusion, the role of the 24/7 contact points network is still important in facilitating the expedited international cooperation between the criminal justice authorities of Parties to the Budapest Convention. However, further development of the network is essential for it to remain a viable and active channel of cooperation, especially in view of expanding membership of the Convention and new developments facilitating international cooperation.

Contact

Cybercrime Division
Council of Europe
Strasbourg, France
cybercrime@coe.int

Appendix 1

Meeting agenda

17 July 2018

2018 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

Strasbourg, France, 11 (AM) July 2018

Palais de l'Europe,
organised by the Secretariat of the Cybercrime Convention Committee with the support of Cybercrime@Octopus, GLACY+, iPROCEEDS, Cybercrime@EAP and Cyber@South projects

AGENDA

11 July 2018	
8h30	Registration
9h00	**Opening session**
9h15	**Introductory panel: Review of the results of the 2017 meeting of 24/7 contact points and follow-up given** Participants will discuss the progress made following the previous meeting of 24/7 contact points.
9h45	**Templates for requests for data** Participants will take note of the templates for data requests as prepared by the T-CY and will discuss on how to make best use of these templates.
10h15	**Production orders for subscriber information related to dynamic IP addresses** In the light of a recent judgment of the European Court of Human Rights (Benedikt v. Slovenia) participants are invited to discuss whether different rules apply in their country for ordering a service provider to produce subscriber information related to dynamic versus static IP addresses.
11h00	*Coffee break*
11h15	**Cooperation of 24/7 contact points with service providers in other jurisdictions** Participants are invited to share their experience with regard to the following questions:

	– What is the overall trend regarding their cooperation with multi-national service providers? – Recent examples (case studies) of such cooperation? – What are the implications of the EU General Data Protection Regulation (applicable as from 25 May 2018) on cooperation with service providers? – Are or should 24/7 points of contact under the Budapest Convention also be the single points of contact for cooperation with providers: advantages/disadvantages? Participants are furthermore invited to exchange views on the proposed Regulation on production and preservation orders as well as the recently adopted US CLOUD Act.
12h30	**Conclusions**

Appendix 2

List of participants

17 July 2018

2018 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

Strasbourg, France, 11 (AM) July 2018

Palais de l'Europe,
organised by the Secretariat of the Cybercrime Convention Committee with the support of Cybercrime@Octopus, GLACY+, iPROCEEDS, Cybercrime@EAP and Cyber@South projects

LIST OF PARTICIPANTS