www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

2019 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

The Hague, Netherlands, 8 October 2019

Summary Report

The Secretariat of the Cybercrime Convention Committee (T-CY) with the support of Cybercrime@Octopus, GLACY+, iPROCEEDS, CyberSouth and CybercEast projects organised the third annual meeting of the 24/7 Network of contact points under the Budapest Convention on Cybercrime, on 8 of October 2019 at the Europol Headquarters in The Hague, Netherlands.

The meeting was built on the outcomes of the previous ones with the aim to reinforce the functioning of the Network to address the challenges of international cooperation on cybercrime and electronic evidence.

The meeting gathered 53 participants representing the contact points from the following countries: Albania, Argentina, Armenia, Azerbaijan, Belarus, Belgium, Bosnia & Herzegovina, Cabo Verde, Chile, Costa Rica, Costa Rica, Czech Republic, Denmark, Dominican Republic, Finland, France, Georgia, Ghana, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Mauritius, Moldova, Montenegro, Morocco, Netherlands, North Macedonia, Norway, Philippines, Poland, Romania, Senegal, Serbia, Serbia, Spain, Sri Lanka, Tonga, Tunisia, Turkey.

Most of the participants were attending the meeting for the first time, as they were either recently mandated with the responsibilities of the 24/7 contact point or representing new members of the Network. The meeting gave them an introduction to the challenges of the organisation and function of the Network and to learn from the best practices of other members.

The meeting was an opportunity for the representatives of the Parties and Observers to the Budapest Convention to discuss about the use and benefits of the Network, the challenges faced when dealing with preservation requests, cooperation with local and multi-national service providers and the MLA process.

Furthermore, examples were provided of criminal investigations where the Network was used to facilitate international cooperation and to progress in investigations and prosecutions as well as examples of the efficiency of the Network.

The first session started with a review of the results of the previous meeting along with the presentation of the process of updating of contact details of the Directory of 24/7 contact points as a means to test the reactivity of the members of the Network. It was agreed that any changes in the contact details of the members should be immediately notified to the Council of Europe for further dissemination within the Network. Also, every six month a ping test will be conducted by the Council of Europe to test the responsiveness of the 24/7 contact points.

With regard to the information contained in the Directory, one proposal was made to include also information on data retention periods in Parties, as this might be useful information when considering sending preservation requests. Although this information is relevant, and countries could be requested to provide it, the Directory might not be the best place to keep it for practical reasons. (For the US it will be impossible to have such data considering the large number of Internet Service Providers and the changes on their data retention policies on regular basis). One of the solutions voiced by some of the Parties in the meeting was setting up of an online secure portal, in which details of 24/7 point of contacts could be updated; other ideas included the common email domain for the entire Network managed by the Council of Europe.

Feedback from participants was requested as regards the use of the templates for preservation of data and MLA requests for subscriber information established based on the articles 29, 30 and 31 of the Budapest Convention and agreed within T-CY meeting from July 2018.

While the issue of the volume of information required to be filled in the templates was raised as a challenge, some countries highlighted the need of detailed information to understand the context of the case and what is actually requested. The information to track down the requests is also appreciated as being useful.

In the end, not much feedback was provided by participants which could lead to the conclusion that a better promotion of the templates is needed as they are useful instruments to help frame the requests and to facilitate the cooperation through the Network. This should be taken up further by the Council of Europe and considered for activities implemented under cybercrime capacity building projects.

The topic of the creation of the secondary contact point was touched upon. Recently, several countries requested advice on this matter and explanations were given about the functioning of the Network. It was highlighted that the decision to designate a secondary contact point belongs to countries, but a coordination mechanism should be put in place in case this is created and clear distinctions between the competences of the two contact points should be drawn in view of the need to complement each other.

New members (Argentina, Cabo Verde, Morocco, Tonga, Philippines and Ghana) briefly introduced their challenges when setting up and assigning responsibilities to the 24/7 contact point.

The presentations provided during this session made it obvious that the responsibilities of the 24/7 contact point should be clearly defined in national legislation or internal rules, and the internal promotion of the role of the Network within the countries will help to improve international cooperation.

In this respect, Council of Europe offered to provide support in advising about the process of establishing the 24/7 contact point as well as training for the staff assigned to it.

One session was dedicated to best practices and examples of cases (Republic of Moldova, Norway and Dominican Republic) where the use of the Network in exchanging information and data

assisted to successful conclusion. The importance of the 24/7 Network was emphasised in regard to the operational cooperation and the benefit of being a specialised Network with its staff attached mostly to the specialised units on cybercrime at the police or prosecutors.

This opportunity was also taken to invite countries to provide examples of the operational use of the Budapest Convention on Cybercrime and its tools in criminal investigations.

The third session focused on the topic of international cooperation and challenges of data retention, preservation of data, cooperation with multi-national service providers and MLA process.

France, Romania and Netherlands presented the way 24/7 contact points work in these countries and their practices when it comes to the preservation of data and cooperation with service providers.

The representative of a Dutch service provider introduced their perspective in cooperating with law enforcement underlining the need for trust and communication as basic grounds for developing a strong public private partnership.

Other countries outlined the importance to regulate the organisation and role of the 24/7 contact point in the national law and shared their experiences in cooperating with multi-national service providers.

Differences in the implementation of the data preservation provisions and related practices were highlighted. The way forward should be the full implementation of the provisions of the Budapest Convention on expedited preservation (articles 16, 17, 29 and 30) as well as on production orders (article 18).

The Second Additional Protocol to the Budapest Convention aiming to speed up the process of international cooperation by allowing authorities from countries to address requests directly to service providers in another jurisdiction is likely to bring new responsibilities for the 24/7 Network.

Europol and Interpol presented their instruments for supporting international cooperation on cybercrime and exchange of electronic evidence. The need for a multidisciplinary approach has been emphasised and their primary focus towards the support of operational cooperation.

The G7 representative introduced their 24/7 Network and expressed the support for the cooperation with the Network established under the Budapest Convention. He also advanced the proposal for a meeting the next year to be organised jointly by the G7 and Budapest Convention Networks.

Joining Budapest Convention and the implementation of its tools are also supported by G7 as a necessary framework for the countries to be equipped with legislative instruments to fight cybercrime and ensure international cooperation.

The last session was dedicated to responsibilities and functioning of the Network and how to increase its efficiency. Participants were invited to share their thoughts and national experiences in regard to the responsibilities, availability and proactivity of the Network.

In order to avoid delays and miscommunications between the members it was strongly recommended that any urgent request to be followed by a call to ensure it is properly executed. Likewise, acknowledging receipt of the request and confirming the starting of the execution of the request will be welcomed.

The requests and answers should be provided through the same channel for international cooperation not to create confusions among the members and hamper the process.

There are different practices for the requests received not from the official contact point (official email account) - while some countries are considering them, others are requiring the requests to be resent by using the official contact details.

For the requests received outside working hours, it was advised to check the contact details communicated by the members which might different from the contact details to be used for working hours and to properly use them.

The proactivity of the members of the Network was encouraged when it comes to the replies and taking necessary steps to execute a request. Likewise, the promotion of the Network at the national level is necessary to ensure its use to the maximum extent.

At the end of the meeting proposals were sought on how to improve the functioning of the Network and based on the discussions during the different sessions and additional proposals made by the participants, the following recommendations can be drawn:

- The organisation, role and responsibilities of the 24/7 contact points should be regulated by law or internal norms.

- The preservation powers under the Budapest Convention need to be implemented directly into the national legislation in order to increase efficiency and clarity in terms of execution of the requests.

- The templates for requesting data developed by the Council of Europe should be promoted and used to the maximum extent in order to facilitate cooperation within the Network.

- The creation of a secure portal for 24/7 contact points to keep the contact details up-to-date and allow easy access to them may be considered.

- To collect information on the data retention period from the Parties and to share it with the members of the Network.

In conclusion, the 24/7 contact points Network is an important channel to facilitate the international cooperation among Parties to the Budapest Convention and can play an important role in the new framework of international cooperation. However, there is still room for improvement when it comes to the use of the Network in practice and the integration of new members.

Contact

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

PROGRAMME OUTLINE (DRAFT)

8 October 2019	
8h30	Registration
9h00	**Opening session**
9h15	**Introductory panel: Developments since the 2018 meeting** • Review of the conclusions from the previous meeting • Directory of 24/7 contact points • Templates for data requests • Secondary 24/7 contact point • Progress made and follow-up given by participants
10h45	*Coffee break*
11h00	**Best practices used by the 24/7 contact points** • Countries are invited to share recent examples where the Network facilitated the cooperation and sharing of data/evidence and how the Budapest Convention was used as an operational treaty
12h30	*Lunch break*
14h00	**International cooperation challenges faced by the Network** • Expedited preservation requests of stored computer data (data retention vs preservation of data, subscriber vs traffic data) • Cooperation with local service providers • Cooperation with multi-national service providers • Facilitating MLA requests • Instruments for international cooperation (Europol) • Cooperation with the 24/7 Network of Interpol (TBC) • Cooperation with G7 Network
15h45	*Coffee break*
16h00	**How to increase the efficiency of the Network** • Responsibilities and availability of the 24/7 contact points • Proactivity of the Network (feedback/reminders for assistance requests) • Promotion of the Network and secure communication channel • Resources and training needs for the staff
17h30	**Summary and the way forward**