www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

2020 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

26 November 2020
-Online-

Summary Report

The Secretariat of the Cybercrime Convention Committee (T-CY), with the support of Cybercrime@Octopus, GLACY+, iPROCEEDS, CyberSouth, and CyberEast projects on 26 November 2020 organised the fourth annual meeting of the 24/7 Network of contact points established under the Budapest Convention on Cybercrime. Due to the COVID-19 pandemic it was held online.

Building on the outcome of previous meetings, it focused on the roles and responsibilities of the 24/7 Network, the instruments and resources required by contact points, as well as the additional responsibilities that contact points may need to assume under the future Second Additional Protocol to the Convention.

The meeting gathered around 100 participants representing the contact points of the following countries: Albania, Argentina, Armenia, Azerbaijan, Belarus, Belgium, Bosnia & Herzegovina, Cabo Verde, Chile, 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, Spain, Sri Lanka, Tonga, Tunisia, Turkey, and the USA.

The session was moderated by Virgil Spiridon, Head of Operations at Cybercrime Programme Office (C-PROC) and responsible for the management of the Network on behalf of the Council of Europe. The introductory panel covered recent progress in relation to the Network. A series of related activities were mentioned, including the capacity-building activities on the use of templates by contact points, the survey by the CyberEast project on data retention provisions in Parties, the online regional workshops organised by the Glacy+ project on the establishment and functioning of 24/7 contact points, and the assessment of the 24/7 contact points of Serbia and Albania. Lastly, the contribution to the webinar organised by the EU Commission to support the EU Member States in implementing the Directive on attacks against informatic systems by setting up 24/7 contact points, was outlined as a good opportunity to introduce the benefits and best practices of the Network established under the Budapest Convention.

Adding more details on these achievements, Giorgi Jokhadze, project manager of the CyberEast project, introduced the outcome of the survey on data retention provisions. His intervention was followed by Matteo Lucchetti, project manager of the GLACY+ project, who shared with participants the main conclusions of a series of workshops on functioning of the Network organised under this project.

Thereafter, the topic of the Directory was discussed along with the need to update and disseminate the contact details of 24/7 contact points (institution, address, communication tools, availability, language, instructions) as a matter of urgency. The Directory comprises 65 members, Parties to the Budapest Convention; in the course of the last twelve months nine updated versions had been shared with the members of the Network.

The benefits of having the organisation, role and responsibilities of the 24/7 contact point regulated by law or internal norms and the use of the templates for preservation and Mutual Legal Assistance (MLA) requests developed by the Council of Europe were emphasised by participants.

At the end of the first session, the new members of the Network, Columbia and San Marino, shared information on their organisation and responsibilities, as well as their internal capacities.

The second session looked at the roles and responsibilities of the 24/7 Network. The first focus was on provisions related to the preservation of data, which are not fully implemented in all Parties, and confusion persists on the difference in terminology and application between expedited preservation and data retention. While preservation refers to all categories of data and needs to be implemented directly into the national legislation in order to increase efficiency and clarity in terms of execution of requests, data retention covers limited data and applies only to telecommunication providers.

	Expedited preservation (Articles 16 and 29 Budapest Convention)	**Data retention (Former EU Directive)**
Aim	Provisional measure to preserve volatile electronic evidence to allow for time for formal measures to obtain evidence	Ensure that data is available for investigation, detection and prosecution of serious crime
Specified/ automated	Specific order for specified data	Automatic retention of data by service providers
Type of data	Any data (including content data)	Traffic and location data and subscriber information (not content data, nor destination IP addresses, URLs, email headers, or list of cc recipients)
Purpose limitation	Any crime involving electronic evidence	Serious crime
Addressee	Any physical or legal person (not limited to service providers)	Service providers
Time period	Flexible: 90 days (renewable)	Specific retention period (6 to 24 months - to be specified in domestic law)

The recent decision of the Court of Justice of the European Union of 6 October 2020, which confirmed that EU law precludes national legislation requiring "a provider of electronic communications services to carry out the general and indiscriminate transmission or retention of traffic data and location data to combat crime in general or of safeguarding national security." In case a Member State faces a severe threat to national security, it may derogate from the obligation to ensure the confidentiality of data for a period that is limited in time to what is strictly necessary, but which may be extended if the threat persists. Thus, the implications of this decision remain to be seen, in particular with regard to "the targeted retention of traffic and location of data".

This was followed by interventions and sharing of experience and good practices by participants.

In this regard, Australia stated that their provisions on data preservation are fully implemented and that the templates are followed, and listed the authorities responsible for collecting evidence. The Turkish representative stated that they will seek to change the national legislation regarding the preservation of data to permit a clearer process. Tunisia's representative elaborated on their development of the draft bill on cybercrime, and on the legislation already have in place related to data preservation. Lastly, he expressed Tunisia's interest in further cooperation with the G7. The delegate of Chile stated his view on the need to increase cooperation on the matter, followed by the Georgian representative, who also mentioned his vision of an increased proactivity within the Network. The UK continued by explaining their internal capacities, while the Argentinian delegate discussed collaboration with Internet Service Providers.

The delegate of Iceland brought up the problem of international preservation requests that are not followed by MLA requests. Preserved data can be retained for 90 days, unless otherwise provided by the law. According to their national legislation, if no MLA follows within this period, the preserved data shall be deleted and one solution to overcome the loosing of data was proposed by Serbia for opening a domestic criminal investigation, especially when bullet proof hosting is involved.

The representative of the Netherlands shared that in their case, data preservation equals access to preserved data if the request mentions the MLA process will follow.

At the end of the second session, Ioana Albani, COE expert, talked about the new legal tools to be introduced by the Second Additional Protocol (SAP) to the Budapest Convention. The Second Additional Protocol aims to speed up international cooperation by allowing authorities from countries to address requests directly to service providers in another jurisdiction, and is likely to bring new responsibilities for the 24/7 Network. Some of its new provisions will include video conferencing, joint investigation teams and investigations, expedited disclosure of stored computer data in an emergency, a direct request to a registrar in another Party, data protection safeguards, and others.

Furthermore, she elaborated briefly on art. 35 of the Budapest Convention and the novelty introduced by the new protocol. This would cover the expedited disclosure of data in an emergency which is the legal basis for obtaining immediate assistance for expedited discloser of specified, stored computer data without a request for mutual legal assistance. It has limited application to emergencies as defined with the aim to provide an expedited procedure of assistance requests made in emergency situations. Next to its usual content, it would require having a description of facts to demonstrate that there is an emergency and how the assistance sought relates to it. Moreover, there would be an obligation to ensure that the designated contact of a Party is available 24 hours and a 7-days-a-week basis for responding to the request. To accommodate diverse legal systems, the text also allows flexibility on the path for the transmission of such requests.

The third session focused on the instruments and resources required by 24/7 contact points. A phone response should follow requests through the 24/7 Network and this proactivity 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 needed to ensure its use to the maximum extent and not only for the benefit of specialised cybercrime units.

Following this, the main benefits of the templates for preserving data and MLA requests for subscriber information established based on articles 29 and 31 of the Budapest Convention were

outlined: they introduce an uniform structure of requests; they contain minimum data for execution of the requests; they reduce the time for processing of the requests; they provide further guidance on the internal processes and they link the requests for preservations and MLA for subscriber information. The Parties can decide to either use them or develop their own forms based on these templates. The templates for requesting data developed by the Council of Europe should be promoted and used to the maximum extent to facilitate cooperation within the Network.

Participants were then invited to step forward and share their thoughts and national experiences concerning the templates. One representative from Philippines shared that in their case, they make full use of the templates, being also proactive in the means of communication. One delegate from the Dominican Republican stated that they find the MLA process cumbersome and currently they are drafting legislation that would ease the procedure.

On the next topic of the agenda related to training, the Council of Europe offered to provide support in advising about establishing a 24/7 contact point and training for the team assigned to it. The staff dealing with contact points matters should have specialized knowledge of the procedures to be taken once a request has been received. Usually, contact points are cybercrime or international cooperation specialists.

When it comes to the internal procedures for processing requests for data, the 24/7 contact point's responsibilities should be clearly defined and the internal promotion of the role of the Network within the countries will help enhance international cooperation. A written procedure to define the steps to be followed when receiving requests is strongly encouraged. For instance, once the request is received and before getting approval for its execution, inquiries in existing data bases are to be conducted in order to identify connections with other requests or domestic criminal investigations. These internal procedures are critical when there are two contact points and a coordination mechanism needs to be in place in order to avoid duplication and not to confuse the requesting parties.

On these topics, the representatives from Romania and Serbia took the floor and shared their internal practices. In Romania, for example, the promotion of the contact point and the training of the staff are taking place in different events organised by the specialized unit on cybercrime with regional offices and other departments from the police. Since there are two contact points, the internal coordination takes place and a common e-mail address was set up for receiving international requests. In Serbia, there are two contact points and the prosecutor is leading the investigations. Furthermore, there is an increased focus on magistrates and their training for raising awareness on cybercrimes and the procedures for formulating and executing requests for international cooperation.

One of the last topics discussed in the third session was the channels of communication. While this subject was also tackled in the previous year’s meeting, it still poses questions. There was an attempt to approach the problem through capacity-building activities, but there are numerous questions to be answered about data privacy, encryption, and data access before moving ahead with any solution for a dedicated channel for communication for the Network. Giving the new responsibilities of the Network that will be introduced by the SAP, available options will still need to be explored.

Lastly, on the internal awareness process it was acknowledged that the Network is primarily used by specialized cybercrime units and others when needed for access to e-evidence. Internally, there is not sufficient knowledge of the existence and responsibilities of the contact points.

The meeting concluded by drawing the following conclusions:

- The Council of Europe will continue to update the Directory and share it with the members of the Network. Members are requested to provide information on any changes as soon as possible. A new version of the Directory will be released in December 2020.
- A ping test will be conducted in the first part of 2021 in order to test the responsiveness of the Network.
- The Council of Europe will continue to guide new members and other countries requesting support to the establishment and function of the 24/7 contact point.
- The C-PROC will continue through its cybercrime capacity building projects to promote the use of templates for international requests of data and to assist with training activities for representatives of 24/7 contact points.
- New synergies with other Networks will be sought since the main aim is to enhance international cooperation and to make use of the international legal framework.
- The 24/7 Contact Points Network is a valuable channel to facilitate international cooperation among Parties to the Budapest Convention and can play even a greater role within the new framework to be introduced by the SAP.
- The next meeting was proposed for the second half of 2021 in a joint format with the G7 Network.

CONTACT

Virgil Spiridon
Head of Operations
Cybercrime Programme Office
Cybercrime Division, Council of Europe
Bucharest, Romania
virgil.spiridon@coe.int

PROGRAM

26 November 2020	
13h00	**Opening session**
13h15	**Introductory panel: Developments since the 2019 annual meeting** • Outcome and conclusions of the 2019 annual meeting • Directory of 24/7 contact points • Progress made and introduction of new members (San Marino, Peru, Columbia) ***(Inputs from participants)***
13h45	**Role and responsibilities of 24/7 Network** • Preservation of data • Collection of evidence (MLA) • New responsibilities according to the future Second Additional Protocol to the Budapest Convention ***(Inputs from participants)***
14h45	**Instruments and resources required for 24/7 contact points** • 24/7 availability of the contact points • Templates for requests of data • Trained staff • Internal procedures for processing the requests for data • Channels for communication • Internal awareness process ***(Inputs from participants)***
15h30	**Summary and the way forward**