www.coe.int/cybercrime

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

2021 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

24 November 2021

- online –

Summary Report

The Secretariat of the Cybercrime Convention Committee (T-CY), with the support of OCTOPUS, GLACY+, iPROCEEDS-2, CyberEast and CyberSouth projects, on 24 November 2021, organised the fifth 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 also this year.

The meeting focused on the responsibilities of the 24/7 Network pursuant to article 35 of the Budapest Convention, in particular, the provisions on technical advice, collection of evidence, provision of legal information, and locating of suspects, as well as the challenges of implementing new responsibilities under the forthcoming Second Additional Protocol to the Convention and possible capacity building support for the members of the Network.

The meeting gathered around 80 participants representing contact points of the following countries: Argentina, Belgium, Bosnia And Herzegovina, Brazil, Bulgaria, Cabo Verde, Chile, Colombia, Costa Rica, Czech Republic, Denmark, Dominican Republic, Finland, France, Georgia, Hungary, Iceland, Italy, Japan, Latvia, Lithuania, Luxemburg, Morocco, Netherlands, New Zealand, Norway, North Macedonia, Paraguay, Peru, Poland, Romania, San Marino, Serbia, Slovakia, Slovenia, Spain, Sri Lanka, Turkey, the UK, and the USA.

Moderation was ensured by Virgil Spiridon, Head of Operations at Cybercrime Programme Office (C-PROC) who is also responsible for the management of the Network on behalf of the Council of Europe.

The first session started with a brief overview by the moderator on his role within the Network and Directory, the topics and outcomes of the previous annual meeting of the Network on 26 November 2020 and capacity building support provided since then by the Cybercrime Programme Office (C-PROC). This introductory session also covered the progress made during 2021 in relation to the Network, including support provided to countries willing to join the Budapest Convention (Tunisia, Brazil, South Africa) to the establishment of their national 24/7 contact point, support to strengthening 24/7 contact points in the Parties to the Budapest Convention interested in establishing a second contact point, as well as promotion of the forthcoming Second Additional Protocol to the Convention and the new responsibilities that it entails for the Network. Lastly, activities jointly organised with INTERPOL were explained as a good opportunity to promote tools and channels for international cooperation on cybercrime and e-evidence and to explain the

complementarity of the I-24/7 Network of INTERPOL and 24/7 Network established under the Budapest Convention.

Thereafter, an update on the Directory was given. The Directory is now complete, comprising the currently 66 members that are Parties to the Budapest Convention; Sweden being the latest addition. Since the last meeting five updated versions had been shared with the members of the Network, pointing out that, according to a recommendation received during previous meetings, changes are highlighted when updated versions are shared.

At the end of the first session, Belgium presented the structure and attributions of their 24/7 contact point, the Federal Computer Crime Unit (FCCU), and provided statistics on requests handled by the contact point since January 2021.

The presentation was followed by a question by the representative of the Netherlands regarding the personnel in charge of incoming and outgoing requests related to cybercrime. The Belgium representative stated that FCCU is handling the requests and few staff members are assigned to this task. The representative of the Netherlands further emphasized the importance of having the unit as contact point rather than a staff member to ensure continuity.

The USA representative stressed the capacities required by the 24/7 Contact point in order to properly fulfil its tasks and further capacity building support which might be needed, mainly in the new Parties, where the 24/7 contact point is located in the capital and other regions of the country are hard to reach. It was also added that the US has integrated in its practice the templates for requesting data developed by the Council of Europe.

The UK representative complemented the previous interventions by stating that having a single department handling all international cooperation requests may dilute the competencies of staff. According to their experience, it is best to have a department which covers only cyber related requests. However, having a specialized department on cyber related request depends on the domestic situation and the volume of requests. The UK representative further shared information on their 24/7 contact point organisation and its internal capacities.

The Brazilian representative asked a question related to requests for the preservation of data and the obligation of service providers receiving the order, to notify the user. The Belgium representative answered that their national law prescribes that the provider might be requested not to notify the user.

The representatives of France also described the organisation of their 24/7 contact point and provided statistics on their outgoing (241, out of which 101 were sent to USA) and incoming (115) requests of 2021. They stated that the 24/7 contact point, established under the Budapest Convention, is one of the most expeditious channels of communication, where you may have a dialogue with your counterparts. As regards the issue of service providers, the French authorities rely on voluntary cooperation.

The Belgium representative replied to the last point made by the France stating that in Belgium the situation is the same as in France, the cooperation of service providers regarding preservation of data is done on voluntary basis.

Virgil Spiridon added that in Romania, when a preservation request is received from another country, through the 24/7 contact point, it is necessary to have an order from the prosecutor for the preservation of data by the service provider.

The New Zealand representative also briefly described the organisation and responsibilities of their cybercrime unit. So far, they rely on the G8 24/7 Network and they are also part of the 24/7 Interpol Network. New Zealand has been invited by the Council of Europe to accede to the Budapest Convention on Cybercrime and the Government is currently undertaking the necessary domestic measures, including stakeholder consultations, to complete the accession process including the establishment of 24/7 contact point under the Budapest Convention. Currently they rely on voluntary preservation of data by service providers.

The USA representatives added that, under their legislation, they may send out a letter request to service providers asking them to preserve data related to certain account which is mandatory under their law. What is specific in this process is that they do not need a court or prosecutorial order, and service providers know their obligations and comply with the requests. The data is preserved for 90 days which may be extended upon request. As regards notification, they cannot get a court order to prevent the notification of the user. However, providers, as a matter of practice, do not notify the user in these cases.

The second session focused on the responsibilities of the 24/7 Network, other than the preservation of data. The moderator explained in detail the provisions of article 35 of the Budapest Convention, with a focus on how the Network may be of great use in the provision of technical advice, collection of evidence, the provision of legal information, and locating of suspects.

The representative of Italy proposed the creation of a table form document, which includes all State Parties to the Budapest Convention and may be extended to the members states of the G7 24/7 Network. The document should include information on data retention and relevant legislation and procedures for preservation of data as well as basic information which could be important when an investigation is initiated. The document could be shared among the members of the group after review by the Council of Europe Secretariat.

The UK representative, proposing a similar initiative added that it would be useful to insert general data retention periods in the 24/7 contact point Directory. Therefore, when requests are made for preservation it is often the case that the best identifiable entity linking back to suspect relates to an event happening months or even a year ago. This means either enquiries are sent out to partners to see if the data might still be available or pointless time may be spent for preservations requests when the data was never available in the first instance. Conversely, it will be easier to check the Directory whether preservation is feasible in first instance. He further emphasized that this would be a useful addition to the Directory and proposed the inclusion of data retention periods in the Directory according to national best practice or legislation and regulations.

With regard to this proposal, the representative of the Netherlands mentioned that communication between the 24/7 contact points should be more flexible. Even though, the inclusion of this information (general data retention periods) in the Directory could be of great use in certain cases, it does not include the assistance that may be provided by the contact point in cases where, for example, the data retention period is very short. The representative explained that in the Netherlands the data retention periods differ depending on the service provider. Therefore, from this perspective he encourages direct communication between the 24/7 contact points.

Virgil Spiridon expressed the support of the Council of Europe for the initiatives proposed by the Italian and UK representatives which will certainly provide more information on the legal system of members and on data preservation or retention periods, and if more clarity is necessary direct follow up could take place between members.

Peru's representative shared with participants their experience with the 24/7 Network. They sent out around 30 preservation of data requests, most of them to the USA. They also cooperated with

Malta, Spain, and the Czech Republic. In particular, she praised the expeditious communication between 24/7 members. The Network enabled the prosecution to speedily receive information, without resorting to mutual legal assistance (MLA). With regard to incoming preservation requests, there is no legal procedure to oblige the service providers to preserve data. However, they relied on the provisions of the Budapest Convention in requesting them to preserve the data for 90 days. On some circumstances the multinational service providers on voluntary basis preserve data up to one year period.

The second session continued with the presentation of the representative of the Romanian National Police, on a case of a ransomware attack and how the Network contributed to the investigation by gathering and preserving data in an expedited and reliable manner and enabled the Cybercrime Unit in Romania to identify the suspects and disrupt their criminal activity.

The representative of Latvia had a short presentation on the organisation, capacities and responsibilities of the 24/7 contact point of Latvia, as well as statistical data on incoming and outgoing requests processed during 2021.

The representative of Slovenia introduced the key legislative developments for harmonisation with provision of the Budapest Convention and organisation and capacities of the 24/7 contact point. He also presented the main challenges they are facing, such as the lack of legal instruments to work with the on-line service providers and increased presence of foreign service providers with limited legal representation in Slovenia. He also emphasized that specialised prosecutor on cybercrime needs to be on board, in order to save time for requests needing a prosecutorial order.

The last session covered questions related to the new responsibilities of the Network under the Second Additional Protocol to the Budapest Convention that will be opened for signature in May 2022. The two new responsibilities would cover the expedited disclosure of data in an emergency and emergency mutual assistance.

The participants were invited to share their views on this topic.

The representative of the Dominican Republic stated that the abilities of the State Parties, in implementing the new provisions referred to above, could be complemented by capacity building activities or standard operating procedures or standard templates developed by C-PROC.

Virgil Spiridon welcomed the proposals and recognised the need for further capacity building. He stated that the specific next steps, after the adoption of the Second Additional Protocol, are yet to be discussed in the Cybercrime Division.

The representative of the USA explained how they envisage to handle requests that are made through article 9 of the Second Additional Protocol, which allows for expedited disclosure of data in emergencies by leveraging on the 24/7 Network. Therefore, when there is an emergency request for disclosure of data to USA providers, this is sent through the 24/7 contact point to his office and they work directly with the providers in the USA to obtain that data, which often is data that the US providers are precluded, by law, from disclosing to foreign governments. However, the national law provides for an exception to disclose content data via the US government in case of emergencies.

Providers often have a template that they use which includes questions on the nature of the emergency, threat to health, security, safety, imminency of the threat. The providers are not obliged to provide the information because, it is a voluntary action on their part. The US 24/7 contact point operates as intermediary and if the provider agrees to disclose data to them this will be forwarded to the foreign authority requesting the data.

As for article 10 on emergency mutual legal assistance, in the US it would probably leverage on colleagues from the Office of International Affairs (OIA), which is handling MLA requests. This office should have staff member on duty 24/7 or at least be reachable and able to initiate the process of executing the requests.

The representative of Cabo Verde stated that their 24/7 contact point is actually one person and expressed interest in onsite and practical trainings of the 24/7 contact point, for reinforcing the knowledge on legal tools for international cooperation on cybercrime and e-evidence and learn more about the international best practices.

The meeting concluded by drawing the following conclusions:

- The meeting was a good opportunity to learn about the best practices and challenges faced by the 24/7 contact points.
- The Council of Europe will continue to update the Directory and share it with the members of the Network for ensuring an expedited international cooperation on cybercrime and e-evidence.
- The Council of Europe will follow up on the proposals of Italy and UK for including in the Directory more information on the legislative framework in its members.
- The Council of Europe will continue to work with its members and other countries requesting support to the establishment and function of the 24/7 contact point as well as to the implementation of the new responsibilities pursuant to the Second Additional Protocol.
- The Council of Europe will seek to develop additional tools for facilitating the implementation of the new responsibilities of the 24/7 Network and cooperation with service providers.
- The C-PROC thorough its cybercrime capacity building programmes will continue to provide guidance and training to the members of the Network as well as to promote the use of the templates for international cooperation.

CONTACT

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

PROGRAM

24 November 2021	
13h00	**Opening session**
13h15	**Update on the functioning of the 24/7 Network since the 2020 annual meeting** • Outcome and conclusions of the 2020 annual meeting • Capacity building support for establishing and strengthening of the 24/7 contact points • Directory of 24/7 contact points ***(Inputs by participants)***
13h45	**Making use and benefits of the 24/7 Network** • Operational cooperation • Technical advice • Provision of legal information • Surveys ***(Inputs by participants)***
14h30	**New responsibilities of the 24/7 Network under the forthcoming Second Additional Protocol to the Budapest Convention** • Expedited disclosure of data in an emergency (Gov2Gov) • Emergency Mutual Assistance (MLA) • Follow-up capacity building support ***(Inputs from participants)***
15h15	**Summary and the way forward**