www.coe.int/cybercrime

2024 Meeting of the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime

The Hague, The Netherlands
18 October 2024

Summary Report

The Secretariat of the Cybercrime Convention Committee (T-CY), with the support of the CyberEast+, CyberSEE, CyberSouth+, GLACY-e and Octopus projects, organised the eighth annual meeting of the 24/7 Network of Contact Points under the Budapest Convention on Cybercrime, at the EUROPOL Headquarters in The Hague, The Netherlands, on 18 October 2024.

The 2024 Annual Meeting focused on addressing challenges to collecting electronic evidence and streamlining processes for cooperation with multinational service providers. Moreover, particular emphasis was given to good practices on the internal promotion of 24/7 Contact Points, dedicated staff, available training, internal procedures for handling requests and new avenues for cooperation among the members of the Network.

The Points of Contact (POC) actively participated in the event, contributing to the discussions, and providing updates on their capacities and sharing examples of operations successfully supported by the Network. The meeting was attended by 94 delegates (81 in person and 13 online), collectively representing 59 countries (48 Parties and 11 Observers) and four international organisations.

The 48 Parties that had designated their representatives to participate in the meeting, either in person or online, were Albania, Argentina, Armenia, Belgium, Bosnia and Herzegovina, Brazil, Bulgaria, Cabo Verde, Chile, Colombia, Costa Rica, Côte d'Ivoire, Denmark, Dominican Republic, Georgia, Germany, Ghana, Ireland, Japan, Mauritius, Moldova, Montenegro, Morocco, Netherlands, Nigeria, North Macedonia, Norway, Panama, Philippines, Poland, Romania, Senegal, Serbia, Spain, Sri Lanka, Tonga, Türkiye, Ukraine, the United States of America. The Council of Europe also welcomed its 8 new members: Benin, Cameroon, Curacao, Fiji, Grenada, Kiribati, Sierra Leone, and Tunisia.

The Observers were: Antigua and Barbuda, Barbados, Ecuador, Jordan, Kazakhstan, Kosovo* , Malaysia,

*This designation is without prejudice to positions on status and is in line with UNSCR 1244 and the ICJ opinion on Kosovo Declaration of Independence.

Seychelles, Singapore, South Korea and Thailand. They expressed their gratitude for the valuable insights, shared experiences and approaches on the practices of the 24/7 contact points. This knowledge will benefit them in the process of establishing their 24/7 contact points as they prepare to accede to the Budapest Convention.

The meeting was moderated by Virgil SPIRIDON, Head of Operations of the Cybercrime Programme Office (C-PROC), responsible for the secretariat of the Network on behalf of the Council of Europe. Delegates from the Council of Europe, the European Commission, EUROPOL, INTERPOL, and the G7 High-Tech Crime Subgroup were present and actively contributed to the debates. Furthermore, representatives of service providers such as Google, Kodex, and TikTok were also invited, and they showcased their mechanisms for sharing data with law enforcement agencies (LEAs) in criminal investigations.

In the opening part, EUROPOL's representative underlined the importance of these meetings for strengthening international cooperation and facilitating cross-border access to data. One focus should be on how to become more efficient in obtaining data faster. EUROPOL's high-level expert group on access to data is expected to improve cross-border cooperation between EU member states and third countries; and the importance of the 24/7 Network was acknowledged in this connection. Such cooperation will be further enhanced by the implementation of the European e-Evidence Package[2], the Second Additional Protocol (2AP) to the Budapest Convention as well as the Council of Europe's dedicated capacity building support.

INTERPOL's representative thanked the Council of Europe for being one of their strongest partners. It was highlighted that among the 24/7 Network's main roles were the improvement of communication by offering a fast and secure way of sharing information, while also providing tools and resources to fight cybercrime. There is no universal solution to respond to cybercrime, and by working together we can better protect our communities and make our societies safer. The complementarity of the INTERPOL's 24/7 Network and the 24/7 Network of Contact Points of the Budapest Convention on Cybercrime was recognised.

The representative of the European Commission stressed the crucial role of the 24/7 Network in facilitating international cooperation to fight cybercrime and the future implementation of the European e-Evidence Package. The role of the 24/7 Network and the Budapest Convention is pivotal in assisting countries to tackle cybercrime, providing technical assistance around the clock, and practical guidance for the handling of e-evidence in cross-border criminal investigations. With the 2AP having already been signed by 47 Parties, the 24/7 Network is becoming even more relevant.

The Council of Europe acknowledged the support provided by the European Commission to the promotion of the international legal standards on cybercrime and electronic evidence offered by the Budapest Convention and its 2AP. This support translates also into financial contribution to the joint capacity building projects implemented by the Cybercrime Programme Office of the Council of Europe.

The first session opened with a brief introduction of the participants followed by a presentation by the moderator on the role of the Network, Directory and the outcomes and takeaways of the previous annual meeting, held also at the EUROPOL Headquarters in October 2023. Benefits for new members were highlighted, and this served as a recap for the other Parties. One of these benefits includes the templates developed by the Council of Europe and promoted through the Network. Parties can decide whether to use these templates or they can develop their own.

The support provided by the Council of Europe to the new members was also outlined, as they may need

[2] Regulation (EU) 2023/1543 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings (*O.J.* L 191, 28.7.2023, pp. 118–180);
Directive (EU) 2023/1544 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings (*O.J. L 191, 28.7.2023, pp. 181–190*).

assistance in the process of establishing their 24/7 points of contact, understanding its role and allocating resources.

Next, Daniel CUCIURIANU as a former manager of the 24/7 Network presented a short recap of the outcomes of the responsiveness test conducted on 7 June 2023 which aimed at evaluating the availability of members for real-time assistance requests and assessing the functionality of the email addresses provided. The overall results were positive, indicating a high level of responsiveness from members within a reasonable timeframe. Some examples were shared and discussed with the audience to illustrate the successful outcomes of the exercise. Over 90% of the Parties responded within 24 hours, while all countries responded within 30 hours.

The Network welcomed new members who joined the Budapest Convention last year (Benin, Cameroun, Cote D'Ivoire, Fiji, Grenada, Kiribati, Sierra Leone, Tunisia) for which dedicated activities were organized to support them. Some of the members took the floor to share their experience, which could serve as good practice for new members.

The Philippines shared their experience related to a request received from the Spanish counterpart in May 2024, following an ongoing investigation conducted on online child sexual exploitation and abuse (OCSEA). This was linked to basic subscriber information connected or related to online sales or distribution of different products. The Philippine authorities collaborated effectively, and the information requested was provided in due time to Spanish authorities.

The moderator of the meeting underscored the need for Parties to act quickly upon request, acknowledging receipt, and send notifications promptly as there may be ongoing sensitive transnational investigations relying on this data.

Tunisia's representative, one of the newest Parties, had an intervention, mentioning their willingness to cooperate with other Parties. Their Ministry of Interior will coordinate with the Ministry of Justice regarding the procedures for handling the requests of the Parties, based on their nature. National legislation will continue to be harmonised with international standards and international cooperation is among the priorities.

Fiji's representative offered more insights regarding the geopolitical situation of the country. This country has been Party to the Budapest Convention since 2024. They are in the process of establishing their 24/7 contact point. They have a hybrid system where police forces do all the investigations and prosecutors only do prosecutions. Further support in the organisation and functioning of the 24/7 contact point will be provided by the Council of Europe as has been discussed in June with the country T-CY representative.

Kiribati also took the floor and provided updates on the status of the cybercrime situation in the country (legislation, cases, and capacities).

Grenada has been a new member since June 2024. They are a developing country, facing cybercrime incidents mostly originating from outside their jurisdiction. Grenada's representative mentioned they were looking forward to international cooperation and the relevance of data obtained from foreign jurisdictions. Their Computer Emergency Response Team (CERT) has been in place since 2019, and inputs from countries was requested in relation to their role in the cybercrime investigations.

The Head of Operations of C-PROC reminded the members of the Network that when setting up the 24/7 point of contact the approach should be to allocate dedicated staff, who is available 24/7 and backed up whenever necessary. Furthermore, the Council of Europe will continue to develop capacity-building activities in support of the Network, and dedicated workshops are also in the pipeline for the near future (Benin, Grenada, Fiji, Kazakhstan, Vanuatu).

The Council of Europe briefly introduced the CYBOX online platform for exchange, training, and resource sharing on cybercrime and electronic evidence. This tool will facilitate online activities, mainly trainings,

and will be offered free of charge to countries and institutions cooperating with the C-PROC and interested in using it. It is a restricted access platform. The primary CYBOX beneficiaries are criminal justice authorities and their respective training institutions (law enforcement academies, judicial academies, etc.) The 24/7 Network will have a dedicated space on this platform (24/7 POC tenant), and it will be further used for communication with the members of the Network and for hosting the Directory. It will also serve as a repository of training and other reference materials on cybercrime and e-evidence.

Another release was the Cyber Skills sharing programme focusing on 30 participating countries (GLACY-e, CyberSEE, CyberSouth+ and Octopus projects). The process of application, categories of professionals and the draft calendar were briefly explained. More information will be available at the beginning of next year through focal points or national coordinators of the countries covered by the above-mentioned projects.

Costa Rica's representative emphasised the crucial role in the fight against cybercrime of their Contact Points from the Prosecutor and the Police, who work closely at the central and regional level for the benefit of the criminal investigations and prosecutions of cybercrime and other offences involving electronic evidence. A mechanism was put in place to ensure efficiency and a shorter time response to the incoming and outgoing requests handled by the 24/7 POC. Proactive investigations are underway to request subscriber information and good collaboration with the USA, France, Albania was outlined.

Ukraine's representative stated they started legislative changes in order to enable the Security Service to become a second point of contact for the 24/7 Network, but the process is taking longer due to other priorities in the country. There are many key players in cybersecurity, including the department for preventing, countering national threats and critical infrastructure. Taking into consideration the current situation and the ongoing war with the Russian Federation, international collaboration and e-evidence are becoming more vital. Efforts are made to document evidence of Russian war crimes, including for submission to international courts. Cyber-attacks are increasing in number and are becoming more complex, targeting critical infrastructure and vulnerable networks of civilian infrastructure. The crucial role of private companies such as Meta, Google, was also highlighted, however international framework for cooperation must be reinforced aiming to allow for quickly access to data from other jurisdictions.

Chile's representative's feedback on the 24/7 Network was positive, describing it as an excellent experience and thanking other Parties such as Germany, the USA, the Netherlands for their cooperation. The Public Prosecutor's Office leads the investigations and that is why the national 24/7 POC is located there. There is a dedicated article for data preservation added into the national legislation in 2023, and based on that service providers can be asked to preserve the data. The preservation is valid for 90 days, with a maximum one-month extension. There is a single point of contact for the cooperation with the internet service providers and every request must go through the national cooperation unit. One ongoing investigation about a fraudulent online trading site asking over 100 victims to invest money (100 million dollars in prejudice) was showcased and the meeting was used as an opportunity to liaise with other countries for identifying any nexus.

Ghana's representative shared the domestic model for setting up the 24/7 contact point for the benefit of the new Parties. In this respect, the internal standard procedure put in place for handling the requests was presented.

Belgium's representative underlined the importance of allocating knowledgeable staff in charge of handling the requests of international cooperation coming through different channels, including the 24/7 Network and the difficulty in progressing in the investigations/prosecutions if access to data is not granted on an expedited basis.

The meeting continued with an in-depth presentation of the CYBOX platform offered by the Council of Europe. As previously mentioned, this will be a space to collaborate effectively and support the 24/7 Directory by being an exclusive area for the contact points. Among the main features are real-time access and customisation, reports and activities section, repository, trainings, and other

resources. The contact points will need to register on the platform once the 24/7 POC tenant is set up. Further information will be shared within the Network in due time.

The third session was dedicated to the cooperation between LEA and private companies (Google, TikTok and Kodex).

Google has different legal subsidiaries, thus it is important to check which entities to contact when requesting information. Google Ireland Ltd. covers Europe and Switzerland and Google LLC covers the USA and the rest of the world. The mutual legal assistance requests (MLA) are different for the USA and the European countries. When preservation requests are to be sent two mechanisms could be used, via Law Enforcement Response System (LERS) or by email. Some important elements to be considered when drafting a request were presented. Template for specific emergency disclosure (EDR) can be downloaded from the Google website. In addition, some useful links can be found online for reporting abuse, product help centres, privacy policy.

The Philippines' representative inquired about the applicable laws for requesting data. Google clarified that the legislation varies depending on the country. For example, EU countries are centred around the GDPR, while the USA revolves around some Cloud Act agreements.

Chile's representative asked for more clarification on the replies received from Google to their requests, as sometimes they don't have the necessary knowledge to interpret it, being not very intuitive. Google can provide trainings for LEAs and can be always contacted for clarifications. Google is working on giving access to more countries to LERS.

TikTok's representative assured Parties of the company's commitment to building trust with LEAs in different regions. They have 3 teams in place, one for outreach, one ERT (emergency) and one LERT (response) for law enforcement support. ERT operates on a 24/7 basis and LERT can be contacted for any request that is not related to an imminent threat. There's also another child safety team which operates on 24/7 basis. The relationship with LEAs is based on education and knowledge sharing, facilitating open communication. Similar to Google, they respond to various requests: MLA, EDR or other legal requests. For the preservation requests, a court order is not needed, a letter from the head of unit from Police suffices and it should be signed and formulated in English. On the other hand, for requests related to the content of communication, a legal process, court order or search warrant is needed. In terms of managing content moderation on disinformation/misinformation, TikTok has developed 2 departments.

Kodex representative presented their mechanism which is a one-stop shop portal for various companies to use as a line of communication between themselves and LEA. It is customisable to be user-friendly and LEAs are verified during the sign-up process. On the landing page, users can see the members the portal being constantly extended to other companies joining. Kodex supports law enforcement agencies in the face of cyber threats and in preventing law enforcement email compromise (LEEC). There are more than 10K validated agencies and 120 countries. Every company has a different process in submitting requests, and it is worth mentioning that LEAs can also directly contact the companies.

Ghana's representative had an intervention, mentioning they had been using Kodex a lot, especially for cryptocurrency investigations and the registration process on Kodex platform took few months. Kodex replied and explained that this process is under development and the registration/validation process will be improved in the near future.

The SIRIUS project, which is the result of close cooperation between EUROPOL and EUROJUST was introduced along with the tools and channels developed within the project for facilitating the access of the criminal justice authorities to e-evidence during criminal investigations. In this respect, a platform was developed for providing assistance to competent authorities in the process of requesting disclosure of data from companies established outside their jurisdiction. There are around 8K users from LEA and judicial authorities registered on their platform and useful documents (guidelines, Standard Operating Procedures, templates, tools, or forums) for guiding in the process of reaching out to different internet service providers

are stored there. Guidelines developed on MLA with a focus on e-evidence are also available. In the long term, the aim is to become a global project and cooperate with partners from outside Europe which is limited now only to the countries that have agreements of cooperation in place with EUROPOL.

The representative of the US DOJ (G7 high-tech crime Network) made a presentation of the Network's functioning. It is managed by the US DOJ and it has as main goal to provide assistance in the preservation of data needed in criminal investigations. The Network is trying to respond to the constant increase of need to obtain electronic evidence from foreign jurisdictions. The Network consists of 101 members, the latest addition being the Seychelles.

The two Networks, established under the Budapest Convention and under G7 complement each other and countries are encouraged to make use of any available channels for international co-operation.

The latest presentation was delivered by INTERPOL's representative who focused also on their 24/7 Network and the international cooperation mechanism in place for assisting member states.

With the existence of different Networks aimed at facilitating international cooperation on cybercrime and electronic evidence, the recommendation was to consider establishing the same staff responsible when a country is part of more Networks.

As a wrap-up, the Annual Meeting of the 24/7 Network is primarily useful for its members in filling in some gaps with information, establishing contacts, learning about the national promotion of the POC, and sharing successful stories.

The meeting concluded with several proposals aimed at further enhancing the functioning of the 24/7 Network:

- The Council of Europe will continue to ensure the management of the Network and keep the Directory up to date.
- The Council of Europe will continue to provide support in the process of setting up the 24/7 POC to the countries interested in acceding to the Budapest Convention.
- Coordination will continue with the SIRIUS project to facilitate access to their platform and tools for the Parties to the Budapest Convention.
- Engaging with the countries that expressed interest in further strengthening of their 24/7 POC through targeted capacity-building activities.
- Migration of the Directory of the 24/7 Network, communication with the members and related capacity-building activities to the CYBOX platform.
- Exploring the organisation of a joint event for the 24/7 Networks established under the Budapest Convention, G7 and INTERPOL in view of harmonization of the practices for international cooperation on cybercrime and electronic evidence.

CONTACT

Virgil SPIRIDON
Secretariat of the Cybercrime Convention Committee (T-CY)
Council of Europe
www.coe.int/cybercrime
virgil.spiridon@coe.int

PROGRAMME

Friday, 18 October 2024	
09h30	**Opening session** • Council of Europe • EUROPOL • European Commission
10h00	**Session 1: Updates on the functioning of the 24/7 Network** • Introduction of participants - tour de table • Outcome and takeaways of the 2023 Annual meeting • Directory of 24/7 contact points • Results of the responsiveness test (19 February 2024) • Introduction of new members (Benin, Cameroon, Curacao, Fiji, Grenada, Kiribati, Sierra Leone, Tunisia)
11h00	*Coffee break*
11h30	**Session 2: Capacity building and good practices** • Activities in support of establishing and strengthening the 24/7 contact points • Exchange of good practices on internal awareness process, dedicated staff, training, internal procedures on processing requests and templates • Cooperation in emergency situations: examples of good practice • Introduction of CYBOX • Operational cooperation between members of the Network
13h00	*Lunch break*
14h00	**Session 3: International cooperation challenges faced by the Network** • Cooperation with multi-national service providers • Collection of evidence and facilitation of MLA process • Tools and channels for international cooperation (SIRIUS project)
15h30	*Coffee break*
16h00	**Session 4: Synergies with other Networks** • Cooperation with G7 Network • Cooperation with 24/7 Network of INTERPOL
16h30	*Summary and way forward*