24/7 POINTS OF CONTACT UNDER ARTICLE 35 OF THE BUDAPEST CONVENTION ON CYBERCRIME

Last update: 20/12/2022

1. BACKGROUND

The Council of Europe Convention on Cybercrime (also known as the Budapest Convention), which was opened for signature in 2001 and entered into force in 2004, was the first international treaty to focus explicitly on cybercrime. After 20 years, it remains the most significant one in the area. Currently, 67 countries are Parties to the Budapest Convention, including 26 EU Member States[1].

The Convention's aim is to function as an international framework for the harmonization of cybercrime-related legislation. It aims at facilitating the fight against criminal offences making use of computer networks by:

- Criminalising the conduct pertaining to cyber-related crime;
- Supporting the investigation and prosecution of these crimes by providing necessary procedural tools; and
- Setting up a fast and efficient system for international cooperation[2].

The Budapest Convention is accompanied by an Explanatory Report which is intended to guide and assist Parties in its application.

More information about the Budapest Convention is available in the dedicated SIRIUS Quarterly Review here.

Effectively combating crimes committed by use of computer systems and the effective collection of electronic evidence in relation to all types of crimes often requires very rapid response. Electronic data with potential evidential value can quickly be lost and can either purposefully or unintentionally be deleted with a few key strokes which may take place thousands of kilometers away. Already at the time of drafting of the Budapest Convention it was therefore agreed that then-existing police cooperation and mutual assistance modalities required supplemental channels in order to effectively address the challenges of the computer age[3].

Article 35 of the Budapest Convention provides a tool for **expedited international cooperation on cybercrime and electronic evidence** between the Parties to the Convention[4]. Joining the network established by means of Article 35 is a requirement of accession to the Convention and the network is currently the only one in which Parties have a **legal obligation to provide a 24/7 cybercrime and electronic evidence capability**. The establishment of this network is among the most important means provided by the Convention for ensuring that Parties can respond effectively to the law enforcement challenges posed by computer- or computer-related crime[5].

The text of the Article 35 provides as follows:

1. Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection

[1] https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185. All EU Member States, except for Ireland.
[2] Budapest Convention, Preamble; Explanatory Report, para. 16.
[3] Explanatory Report, para. 298.
[4] https://www.coe.int/en/web/cybercrime/24/7-network-new-#{%22105166685%22:[0,1,2,3]}.
[5] Explanatory Report, para. 298.

The SIRIUS project has received funding from the European Commission's Service for Foreign Policy (FPI) under contribution agreement No PI/2020/417-500. This document was produced with the financial assistance of the European Union. The views expressed herein can in no way be taken to reflect the official opinion of the European Union.

of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:
a. the provision of technical advice;
b. the preservation of data pursuant to Articles 29 and 30;
c. the collection of evidence, the provision of legal information, and locating of suspects.

2. a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.
b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to coordinate with such authority or authorities on an expedited basis.

3. Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

The mechanism established under Article 35 of the Budapest Convention was based upon the experience gained from the 24/7 network created under the auspices of the then Group of Eight[6] (G8, now G7)[7].

The G7 24/7 network, created in 1998, is a point-to-point network for urgent assistance in cybercrime matters which entails the establishment of single, English-speaking points of contact knowledgeable in cybercrime matters, available 24 hours per day, 7 days per week, to all other member nations. Its primary purpose is to preserve data for subsequent transfer through Mutual Legal Assistance (MLA) channels.

2. SCOPE

- **Types of crimes covered**

[6] The G8 was an inter-governmental political forum from 1997 until 2014. It was formed by incorporating Russia into the Group of Seven – or G7 (Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States of America) – and returned to its previous name after Russia was removed in 2014.

Points of contact under Article 35 of the Budapest Convention are designated to ensure immediate assistance in **investigations and proceedings concerning criminal offences related to computer systems and data**, or for the **collection of evidence in electronic form of a criminal offence**[8]. This means that the provision applies either where a crime is committed by use of a computer system, or where a crime not committed by use of a computer system (for example a murder) involves electronic evidence.

3. DEFINING THE TOOLBOX

Article 35(1) of the Budapest Convention requires Parties to establish **points of contact available 24 hours a day, 7 days a week**, which, in accordance with domestic law, can either **assist in or carry out** a number of specific measures, namely:

- The provision of technical advice (Article 35(1)(a));
- The preservation of data pursuant to Article 29 (Expedited preservation of stored computer data) and Article 30 (Expedited disclosure of preserved traffic data) of the Budapest Convention (Article 35(1)(b)); and
- The collection of evidence, the provision of legal information and locating of suspects (Article 35(1)(c)).

The term "**legal information**" is intended to cover any advice to another Party that is seeking cooperation concerning any legal prerequisites required for providing informal or formal cooperation[9].

- **Location of 24/7 points of contact within the national structure**

Parties have the liberty to autonomously determine where to locate the 24/7 points of contact within their own national system[10]. This may be, for

[7] Explanatory Report, para. 298.
[8] Ibid.
[9] Explanatory Report, para. 299.
[10] Explanatory Report, para. 300.

example, within the central authority for mutual legal assistance or within a police unit specialised in fighting computer- or computer-related crime, but other options are also possible depending on each Party's governmental and legal structure. Considering the wide range of measures that points of contact are expected to assist in or carry out, ranging from the provision of technical advice (e.g. for stopping or tracing an attack) to carrying out international cooperation duties (e.g. the locating of suspects), different options are possible and the structure of the 24/7 points of contact network may evolve over time[11].

Furthermore, pursuant to Article 35(2), 24/7 points of contact must be able to facilitate the rapid execution of those functions that they do not carry out themselves. Therefore, for example, if the 24/7 point of contact is part of a police unit, it must have the ability to coordinate expeditiously with other relevant components within its government, such as the central authority for international extradition or mutual assistance and vice versa[12].

In practice, most 24/7 contact points are attached to **specialised police or prosecution services for cybercrime**[13].

The 24/7 network established in accordance with Article 35 of the Budapest Convention is supported by the Council of Europe (CoE)[14].

The CoE, among other things, maintains a **Directory of points of contact**[15] which is regularly updated and shared with members of the 24/7 network. For a list of EU Member States' 24/7 contact points, see the Annex. It is noted that some countries have established two 24/7 contact points. This may include one contact point for law enforcement and one for judicial authorities, or the contact points can be otherwise internally divided and specialised. In these cases, contacting either one will suffice form the perspective of foreign authorities, as any further contact with competent national authorities would be facilitated by the contact point itself on an expedited basis.

Twice a year, the T-CY Secretariat organises so-called "ping" tests in order to verify if the 24/7 points of contact are functional and the provided details are valid.

- **Expedited communication capacity**

Article 35(2) requires each 24/7 point of contact to have the capacity to carry out **communications with other members** of the network on an **expedited basis**[16]. Therefore, one consideration for Parties in designating their respective points of contact is the need to be able to communicate with other points of contact in other languages[17].

- **Trained and equipped personnel**

Article 35(3) requires each 24/7 point of contact to have **proper equipment**. This will generally include up-to-date telephone and computer equipment, as well as other forms of communication and analytical equipment as technology advances[18].

Article 35(3) further requires that personnel forming part of the 24/7 contact point team be **properly trained**. Such training shall cover computer- or computer-related crime and how to respond to it effectively[19].

It is the duty of the Parties to ensure that trained and properly equipped personnel are available in order to facilitate the operation of the network.

In 2014, the T-CY completed an assessment of the functioning of MLA under the Budapest Convention and adopted a set of recommendations[20].

[11] Ibid.
[12] Explanatory Report, para. 301. See also T-CY, *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, 3 December 2014, p. 86.
[13] https://www.coe.int/en/web/cybercrime/24/7-network-new-#{%22105166685%22:[0,1,2,3]}.
[14] Ibid.
[15] https://rm.coe.int/cyber-list-of-competent-authorities-september-2021/1680a3aaae.
[16] Explanatory Report, para. 301.
[17] Explanatory Report, para. 300.
[18] Explanatory Report, para. 302.
[19] Ibid.
[20] T-CY, *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime*, 3 December 2014.

Recommendation 5 covered 24/7 points of contact and stated, among others, that Parties should work towards strengthening the role of 24/7 points of contact, including through ensuring that trained and equipped personnel is available to facilitate the operative work and conduct or support MLA activities and conducting regular meetings and training of the 24/7 network among the Parties[21].

In a 2017 follow-up assessment, it was indicated that almost all Parties took actions to follow the recommendation and all reported that they ensure that trained and equipped officials are available to facilitate the operative work and conduct or support MLA requests involving electronic data[22].

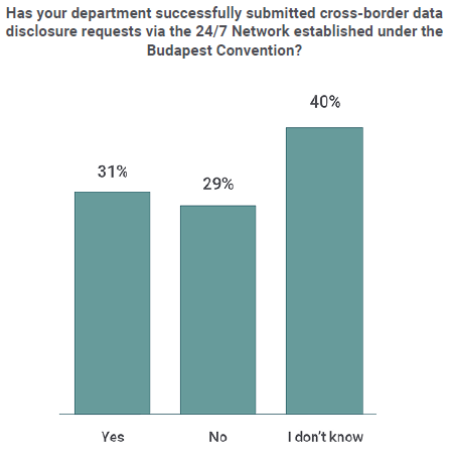
4. SUBMISSION OF CROSS-BORDER REQUESTS FOR DATA VIA THE 24/7 NETWORK IN THE EU MEMBER STATES

As 24/7 points of contact play a role in the submission of cross-border requests for data, EU law enforcement authorities surveyed for the SIRIUS EU Digital Evidence Situation Report 2022[23] were asked about the level of engagement via this channel.

31% of respondents indicated their department successfully submitted cross-border data disclosure requests via the 24/7 network in their investigations in the previous year. This constitutes an increase of 7% from 2020 to 2021.

[21] Ibid, pp. 125-126.
[22] T-CY, *Assessment report on Mutual Legal Assistance: Follow up given by Parties and Observers*, 28 November 2017, p. 15.
[23] SIRIUS EU Digital Evidence Situation Report 2022, December 2022, p. 16. For the methodology used for the purposes of the report, see p. 11.

24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime



However, there seems to be a general lack of awareness about this channel, as 40% of EU law enforcement officers surveyed reported.

5. THE WAY FORWARD

The Second Additional Protocol to the Convention on Cybercrime (Protocol), which was opened for signature to the Parties to the Convention in May 2022[24], will bring new responsibilities for the 24/7 network in order to enhance international cooperation between States, as well as cooperation with the private sector[25].

Specifically, Article 9 of the Protocol provides a basis for cooperation between authorities for the **disclosure of stored computer data in emergency situations**. It permits each Party to utilize their 24/7 points of contact established under the Budapest Convention to both send and receive immediate requests to a point of contact in another Party "seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data" in an emergency situation, **without the need to send an MLA request**[26].

Furthermore, pursuant to Article 10 of the Protocol, Parties may seek **expedited MLA in case of an emergency**. Emergency MLA requests under

[24] https://www.coe.int/en/web/cybercrime/t-cy-drafting-group.
[25] https://www.coe.int/en/web/cybercrime/24/7-network-new-#{%22105166685%22:[0,1,2,3]}.
[26] Protocol, Article 9(1)(b).

24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime

Article 10 of the Protocol may be sent, among other channels, **from the 24/7 point of contact in the requesting country to the 24/7 point of contact in the receiving country**[27].

More information about the Protocol is available in the dedicated SIRIUS Quarterly Review here.

[27] Protocol, Article 10(9).

24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime

ANNEX
LIST OF COMPETENT AUTHORITIES SET UP IN ACCORDANCE WITH ARTICLE 35 OF THE BUDAPEST CONVENTION (UPDATED ON 1 SEPTEMBER 2021)

AUSTRIA

Cyber-Crime Competence Center (Federal Criminal Police Office)
Bundeskriminalamt (Federal Criminal Police Office) at the Bundesministerium für Inneres (Federal Ministry of the Interior) Criminal Intelligence Service
BK 5.2 - Cybercrime Competence Center
Josef Holaubek Platz 1, 1090 Vienna, Austria

BELGIUM

Federal Computer Crime Unit
Konigsstraat 202 A, 1000 Brussels, Belgium

BULGARIA

General Directorate Combating Organized Crime
Ministry of the Interior
133A Tsarigradsko Shose blvd, Sofia, Bulgaria

CROATIA

Cyber Security Department
Criminal Police Directorate – Ministry of Interior
Police HQ, Ilica 335, HR-10000 Zagreb, Croatia

CYPRUS

Office for Combating Cybercrime and Forensic Lab,
Department C Cyprus Police Headquarters, Nicosia, Cyprus

CZECHIA

Police of the Czech Republic National Organized Crime Headquarters
Criminal Police and Investigation Service, Cybercrime Division
P.O. Box 41/NCOZ 156 80, Prague 5, Czechia

DENMARK

Danish National Police Department for International Communication
Polititorvet 14, DK-1780 Copenhagen V, Denmark

ESTONIA

Bureau of Criminal Intelligence
Criminal Police Department, Estonian Police and Border Guard Board

Intelligence Management and Investigation Department Law Enforcement Intelligence Management Bureau (SPOC) Tööstuse 52, 10419 Tallinn, Estonia

FINLAND

National Bureau of Investigation
Box 285, FIN-01371, street Jokiniemenkuja 4 (Vantaa)
Ministry of Justice International Affairs, POB 25 FIN-00023 Government street Eteläesplanadi 10, Helsinki, Finland

FRANCE

Office Central de Lutte contre la Criminalité liée aux Technologies de l'Information et de la Communication – OCLCTIC
Ministère de l'Intérieur French National Police Central Direction of Judicial Police (DCPJ) / French National Cybercrime Unit (Sous-Direction de Lutte contre la Cybercriminalité) DCPJ/SDLC/OCLCTIC
Place Beauvau 75800, Paris Cedex 08, France

GERMANY

National High Tech Crime Unit Federal Criminal Police Office (BKA)
Thaerstr. 11 D – 65193, Wiesbaden, Germany

GREECE

Cyber-crime Division Hellenic Police Headquarters
173 Alexandras Avenue, 11522 Athens, Greece

HUNGARY

International Law Enforcement Cooperation Centre Permanent Service Police
H-1139 Budapest, Teve utca 4-6 A/V/541, Budapest, Hungary

National Bureau of Investigation Cybercrime Department
Aradi utca 21-23 H-1062, Budapest, Hungary

ITALY

Servizio Polizia Postale e delle Comunicazioni
Ministry of Interior
Via Tuscolana 1548, Roma, Italy

General Attorney – Italian Supreme Court
Procura Generale Corte Suprema di Cassazione
Palazzo di Giustizia Piazza Cavour 00193, 00165, Roma, Italy

24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime

LATVIA

1st Unit (Operational cross- border cooperation)
1/4 Ciekurkalna 1.line, LV-1026 Riga, Latvia

LITHUANIA

Serious and Organized Crime Investigation Board 5 (SO5 – Cybercrime)
Lithuanian Criminal Police Bureau
Saltoniskiu st. 19, LT- 08105 Vilnius, Lithuania

LUXEMBOURG

24/7 Network for High Tech Crime
Police Grand-Ducale
CIN – Centre d'Intervention National

Prosecutor's Office of the district
Court of Luxembourg Cité Judiciaire
Permanence Prosecutor's Office
Building PL L-2080, Luxembourg-City, Luxembourg

MALTA

Cybercrime Unit Malta Police Force
Police General Headquarters, Floriana CMR2000, Malta

NETHERLANDS

Landelijk Internationaal Rechtshulpcentrum (LIRC) National Police
P.O. box 11, 3970 AA Driebergen, The Netherlands

POLAND

Cybercrime Division Cybercrime Bureau
National Police Headquarters
Puławska str. 148/150, 02-624 Warsaw, Poland

PORTUGAL

Cybercrime unit of the Judicial Police (UNC3T – SCICIT/ Criminalidade Informática)
Coordinator of Criminal Investigation Police in Portugal Judicial Police
Rua Gomes Freire 174, 1169-007 Lisbon, Portugal

24/7 Points of Contact Under Article 35 of the Budapest Convention on Cybercrime

ROMANIA

Service for Combating Cybercrime
Directorate for the Investigating Organised Crime and Terrorism (DIOCT) within Prosecutor's Office attached to the High Court of Cassation and Justice
24 Calea Grivitei, Sector 1, Bucharest, Romania

Romanian National Police Service for Combating Cybercrime
Directorate for Combating Organised Criminality
Street Stefan cel Mare 13-15, Sector 2, Bucharest, Romania

SLOVAKIA

National Central Bureau of Interpol
Pribinova 2, 81272 Bratislava, Slovakia

SLOVENIA

Sector for international police cooperation
Criminal Police Directorate Slovene Police
Cyber Investigation Unit of Police, Ljubljana, Slovenia

SPAIN

Central Unit on Technological Investigation
Cuerpo Nacional de Policía (Spanish National Police)

Computer Crime Unit Guardia Civil
C/ Salinas del Rosío no. 33-35 28042, Madrid, Spain

SWEDEN

Swedish Cybercrime Centre, SC3
National Operations Department, Stockholm, Sweden