COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Version 29 September 2017
Strasbourg, France

T-CY (2017)2

Cybercrime Convention Committee (T-CY)

Assessment report on Mutual Legal Assistance:

Follow up given by Parties and Observers

Draft prepared by the T-CY Bureau for consideration by T-CY 18
(27-28 November 2017)

www.coe.int/TCY

Contents

Contact
Alexander Seger
Executive Secretary of the Cybercrime Convention Committee (T-CY) Tel +33-3-9021-4506
Directorate General of Human Rights and Rule of Law Fax +33-3-9021-5650
Council of Europe, Strasbourg, France Email: alexander.seger@coe.int

1 Background

Expeditious mutual legal assistance (MLA) is one of the most important conditions for effective measures against cybercrime and other offences involving electronic evidence given the transnational and volatile nature of electronic evidence. In practice, however, mutual legal assistance procedures are considered, in some circumstances, too complex, lengthy and resource intensive, and thus too inefficient.

The Cybercrime Convention Committee (T-CY), at its 8th Plenary Session (5-6 December 2012), therefore, decided to assess in 2013 the efficiency of some of the international cooperation provisions of Chapter III of the Budapest Convention on Cybercrime, with a focus on Article 31 Budapest Convention which provides for "mutual legal assistance regarding accessing to stored computer data" on an expedited basis:

> Article 31 - Mutual assistance regarding accessing of stored computer data
> 1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.
> ...
> 3 The request shall be responded to on an expedited basis where:
> a) there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or
> b) the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

The assessment was completed with the adoption of the Assessment Report by the 12th Plenary of the T-CY on 2-3 December 2014.[1]

The Report comprises a set of recommendations falling under the responsibility of Parties:

Rec 1	Parties should fully implement and apply the provisions of the Budapest Convention on Cybercrime, including preservation powers (follow up to T-CY Assessment Report 2012).
Rec 2	Parties should consider maintaining statistics or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence.
Rec 3	Parties should consider allocating more and more technology-literate staff for mutual legal assistance not only at central levels but also at the level of institutions responsible for executing requests (such as local prosecution offices).
Rec 4	Parties should consider providing for better training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be supported by the capacity building programmes of the Council of Europe and other organisations.
Rec 5	Parties and the Council of Europe should work toward strengthening the role of 24/7 points of contact in line with Article 35 Budapest Convention, including through: a. Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities b. Encouraging contact points to pro-actively promote their role among domestic and foreign counterpart authorities;

[1] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

	c. Conducting regular meetings and training of the 24/7 network among the Parties; d. Encouraging competent authorities and 24/7 points of contact to consider procedures to follow up to and provide feedback to the requesting State on Article 31 requests; e. Considering to establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests; f. Facilitating 24/7 points of contact to play a supportive role in "Article 31" requests.
Rec 6	Parties should consider streamlining the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.
Rec 7	Parties should make use of all available channels for international cooperation. This may include formal mutual legal assistance, police-to-police cooperation and others.
Rec 8	Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.
Rec 9	Parties should confirm receipt of requests systematically and give, upon request, notice of action taken.
Rec 10	Parties may consider the opening of domestic investigation upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA.
Rec 11	Parties should make use of electronic transmission of requests in line with Article 25.3 Budapest Convention on expedited means of communication.
Rec 12	Parties should ensure that requests are specific and complete with all necessary information.
Rec 13	Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are reminded to apply the dual criminality standard in a flexible manner that will facilitate the granting of assistance.
Rec 14	Parties are encouraged to consult with authorities of requested Party prior to sending requests, when necessary.
Rec 15	Parties should consider ensuring transparency regarding requirements for mutual assistance requests, and reasons for refusal, including thresholds for minor cases, on the websites of central authorities.

Parties were invited to follow up on recommendations falling under their responsibility and to report back to the T-CY no later than 18 months on measures taken as to permit T-CY, in line with the Rules of Procedure (Article 2.1.g), to review progress made.

Following a decision by T-CY 15 (24-25 May 2016) "to invite the Bureau to develop and the Secretariat to circulate a request for information on follow up given to Recommendations 1-7 and 9-15 of the MLA Assessment Report, as well as on Recommendation 16 on time periods for data preservation periods", a questionnaire prepared by the T-CY Bureau was circulated to all Parties on 16 September 2016, with a deadline for replies 21 October 2016. By 21 October 2016, 18 Parties had replied to the questionnaire.

T-CY 16 (14-15 November 2016) decided "to welcome the replies to the questionnaire on follow up given by 18 Parties and to invite the remaining Parties and Observer States to provide their replies no later than 15 December 2016".

T-CY 17 (7-9 June 2017) decided to invite Parties and Observers to send comments and to encourage additional Parties and Observers to send replies to the questionnaire to the Secretariat

by 15 July 2017 to permit the Bureau to review the draft report on follow up given to the report on MLA in view of detailed discussion by T-CY 18 (November 2017).

The T-CY Bureau reviewed comments received and prepared a consolidated report in its meeting on 18 September 2017 for consideration by the T-CY.

By 17 July 2017, 40 Parties and 1 Observer State had replied to the questionnaire:

Albania	Finland	Netherlands
Armenia	France	Norway
Australia	Germany	Philippines
Austria	Hungary	Poland
Azerbaijan	Israel	Portugal
Belgium	Italy	Romania
Bosnia and Herzegovina	Japan	Serbia
Bulgaria	Latvia	Slovakia
Canada	Liechtenstein	Slovenia
Croatia	Lithuania	Spain
Czech Republic	Malta	Switzerland
Denmark	Mauritius	Turkey
Dominican Republic	Moldova	United States of America
Estonia	Montenegro	

2 Follow up given by Parties to Recommendations 1 to 15[2]

2.1 Rec 1 – Implementation of provisions of the Budapest Convention

Parties should fully implement and apply the provisions of the Budapest Convention on Cybercrime, including preservation powers (follow up to T-CY Assessment Report 2012).

2.1.1 Overview of follow up given

This Recommendation derived from Parties' belief that the full implementation of the procedural and international cooperation provisions already in the Budapest Convention would greatly assist obtaining evidence internationally.

Most responding States assert that they comply with the Convention's requirements[3]. Some state specifically that their law contains a provision establishing preservation (Albania, Armenia, Australia, Canada, Croatia, Finland, Japan, Latvia, Lithuania, Malta, Moldova, Montenegro, Netherlands, Norway, Philippines, Poland, Portugal, Romania, Slovakia, Spain, United States). [4]

Some States that do not have a legal provision that establishes preservation rely on implicit enforcement powers to carry out preservation (Bulgaria, Czech Republic, Estonia, France). Others are considering writing such a provision into statute or regulation (Azerbaijan, Italy, Slovenia).

A few States require formal mutual legal assistance in order to carry out Article 29 preservation requests or are otherwise not fully in line with the Convention (Hungary, Mauritius and Turkey).[4] Others are in the process of improving their domestic implementation of the convention[5] (Bosnia and Herzegovina, Czech Republic, Liechtenstein and Serbia).

2.1.2 Examples of good practice

Many States follow the good practice of establishing a written preservation provision in domestic law that allows preservation to be executed simply, quickly, and without a court order.

2.1.3 Conclusion

The procedural and international cooperation provisions of the Budapest Convention are crucial to obtaining evidence internationally and should all be fully implemented. In particular, preservation is the most basic, frequently-used and least-intrusive of these tools. Parties should remove impediments to the easy use of preservation powers and strongly consider establishing written

[2] Note: The Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania is supporting Parties and Observer States through a range of projects and activities in the implementation of the Budapest Convention, including in the follow up to the recommendations of the T-CY Report on MLA. These activities are not specifically listed under each Recommendation. Projects are listed in the appendix to this report.
[3] Cyprus, Georgia, Iceland, Luxembourg, Panama, Sri Lanka, "The former Yugoslav Republic of Macedonia," Ukraine, and the United Kingdom did not reply to this question.
[4] For a detailed analysis on the implementation of the provisions related to preservation see the Cybercrime Convention (T-CY) reports:
Assessment report Implementation of the preservation provisions of the Budapest Convention on Cybercrime
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e
Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime : supplementary report
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

preservation provisions in any legally-binding form (statute, regulation, etc.) that is appropriate for their country.

2.2 Rec 2 – Statistics and monitoring the efficiency of MLA

> Parties should consider maintaining statistics or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence.

2.2.1 Overview of follow up given

By this Recommendation, Parties suggested that concrete data about the increasing burdens posed by electronic evidence requests - rather than generalised complaints - might alert policymakers and perhaps attract more resources to the offices that handle MLA requests involving electronic data.

Many States keep statistics for MLA requests involving electronic data[6] and could query existing databases to obtain such statistics, or have new document and case management systems that enable statistics-keeping (Albania, Australia, Azerbaijan, Belgium, Bulgaria, Canada, Croatia, Hungary, Italy, Lithuania, Malta, Mauritius, Moldova, Montenegro, Romania,[7] Serbia, Slovakia, Slovenia, Spain, Switzerland, Turkey, United States). Others are in the process of developing such systems (Bosnia and Herzegovina, Czech Republic, Finland, Netherlands).

Some States affirm that such statistics-keeping is not available or is not possible (Armenia, Austria, Denmark, France,[8] Israel, Liechtenstein, Norway, Poland). In Liechtenstein, the caseload is small enough for it to evaluate efficiency without a database.

Portugal noted, and Germany agreed, that exact statistics about MLA requests involving electronic data are impossible to keep because direct cooperation between judicial authorities does not involve central control points. Direct cooperation is widely cited as a tool for improving cyber-cooperation and very much used between EU member States.

2.2.2 Examples of good practices

Australia: the Central Authority maintains a database of all MLA cases, including those relating to cybercrime and electronic evidence. The database enables the CA to produce statistics about the number of cases in particular categories (including by country of origin, offence type and assistance type). The Central Authority is reviewing its casework management requirements with a view to developing an improved database. The Central Authority also continually monitors and reviews casework practices for responsiveness and efficiency.

Canada: The Central Authority maintains an electronic database of all MLA requests seeking electronic data that have been made by or to Canada, which identifies the nature of the underlying offence, the type of assistance sought and the date processed. This database also allows all relevant documents and correspondence associated to the request to be uploaded for ease of reference.

[6] Cyprus, Georgia, Germany, Iceland, Latvia, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to this question. This footnote was marked for deletion. Since there was no explanation and most similar footnotes were not marked for deletion, the footnote was retained.

[7] Romania - through the prosecutor's office during the investigation stage - keeps statistics for cybercrime MLA only, not for MLA relating to electronic evidence.

[8] France can track the number of cases handled by the Central Authority but not specifically the number of cybercrime and electronic evidence cases.

Malta: the Office of the Attorney General has a database that keeps statistical information about all incoming and outgoing requests for MLA, including offences relating to cybercrime and electronic evidence.

Moldova: the General Prosecutor's Office maintains statistics on all requests for MLA, including those related to cybercrime. Together with the Department for Information Technology and Combating Cybercrimes, the GPO maintains strict tracking of requests related to cybercrime.

Montenegro: the Central Authority uses electronic case management for MLA. This provides statistical data according to different criteria, such as criminal offence, type of MLA, requesting state, and others.

Philippines: The Philippines Department of Justice – Office of Cybercrime (DOJ-OOC) faithfully maintains records/database of incoming and out-going mutual legal assistance requests related to cybercrime and electronic evidence.

Switzerland: statistics are published online (supplying links).

United States: the Central Authority maintains a database for all incoming MLA requests that seek electronic records (whether the request comes in on paper or electronically). The database tracks, among other things, the length of time a request has been pending, communications to and from the requesting state, and each case's resolution. The system can also produce statistics and trends relating to these types of requests.

2.2.3 Conclusion

It seems that most States are able to produce some statistics on MLA requests involving electronic data. It might be interesting to see if these statistics reflect the impression that cybercrime practitioners express – that is, that the system is slow and overburdened. Beyond that, the T-CY could analyse if aggregated statistics could be used in some way. It would be useful if available statistics could be shared with the T-CY.[9]

It may be interesting to see if other States that rely on direct contacts encounter the problem that Portugal raises, namely that this prevents States from keeping accurate statistics.

[9] Note: During the T-CY assessment very few Parties provided statistical data.

2.3 Rec 3 – Allocation of resources

> Parties should consider allocating more and more technology-literate staff for mutual legal assistance not only at central levels but also at the level of institutions responsible for executing requests (such as local prosecution offices).

2.3.1 Overview of follow up given

The premise of this Recommendation was that mutual legal assistance can be slowed or even precluded if officials in the MLA chain are unfamiliar with the technology at issue in a case – they may not ask the right questions or supply the right foundation to support or speed an MLA request.

In general, Parties take seriously the problems underlying this Recommendation. Most are addressing those problems, primarily with training, liaison, and special staffing.[10] The three approaches are often combined.

States are listed below roughly according to the main points that they emphasised in their responses. Such listing does not mean that they are not taking other steps. On the contrary, it seems that States are trying different methods to spread and deepen technical knowledge.

Parties specifically mention:

- Training for officials who work on MLA requests involving electronic data: Australia, Belgium, Bulgaria, Finland.
- Networking or special connections between relevant offices, such as prosecution offices that handle MLA requests involving electronic data and the national cyberpolice: Austria, Dominican Republic, Germany, Hungary, Liechtenstein, Malta, Slovakia.
- Specialised staffing: Albania, Azerbaijan, Canada, Czech Republic, Denmark, Estonia, France, Israel, Japan, Lithuania, Mauritius, Moldova, Norway, Romania, Switzerland, Turkey, United States.

Other States are considering this issue, emphasising specialised training within local prosecution offices, or recruiting technologically-literate staff (Bosnia and Herzegovina, Finland, Poland, Serbia).

2.3.2 Examples of good practices

Australia: the Central Authority trains its officials when they start in the job and thereafter to keep them abreast of developing technologies, including how criminals use them.

Austria: the cooperation between prosecutors and the cyberpolice in the central police office is fast, flexible, and efficient. In addition, each regional court and prosecution office has technical staff who can offer support.

Azerbaijan: technology-literate staff are assigned to handle MLA requests involving electronic data both at central levels and in the institutions that are responsible for executing the requests.

[10] Croatia, Cyprus, Georgia, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to this question. Portugal reported no specific measures taken.

Canada: Recently established a Cyber-Unit within the Canadian Central Authority to increase the level of cyber expertise, to maintain computer-literate staff, and to implement a process that would increase efficiencies and ensure consistency in the review and execution of requests seeking access to electronic data. Ongoing training by cyber experts is provided to members of this unit.
France: in numerous offices of the French government (including in the Central Authority and in Paris, Lille and elsewhere), there are magistrates, officials and dedicated units specialising in cybercriminality, collection of electronic evidence, cyberforensics, and cyberinvestigations.

Israel: the State's Attorney's Office includes an International Department which operates a designated authority on matters of law and technology, and a Cybercrime Department. The Cybercrime Department meets regularly with foreign colleagues and with several Internet service providers.

Japan: in the Supreme Prosecutors' Office and in major District Prosecutors' Offices, technology-literate prosecutors are in charge of cybercrime cases. The Ministry of Justice also promotes the ability of prosecution officials to investigate cybercrime nationwide by providing training on technology used in cybercrime and on electronic investigation methods. Within the national and prefectural police forces, technologically-trained staff are assigned to cybercrime investigations.

Lithuania: MLA requests involving electronic data are handled jointly by prosecutors and investigators who are proficient in the technical and legal issues. The technical collection of the evidence is handled by cyberinvestigators assigned to cybercrime divisions in either the central national police or one of ten local-level police forces. The cybercrime division at national level normally handles high-profile, organised crime and transnational cases.

Switzerland: specialised cybercrime units have been established within the prosecutors' offices at the federal and cantonal levels. There are also specialised prosecutors in the Office of the Attorney General of Switzerland, which ensures that the appropriate legal and technological knowledge related to cybercriminality is available in MLA requests involving electronic data. There are several platforms to ensure the transfer of specialised knowledge within the same canton and between cantons and federal authorities.

United States: as part of its MLA Modernization Project, the US Central Authority has a Cyber Unit whose attorneys and support staff focus exclusively full-time on MLA requests involving electronic data. The Central Authority collaborates with federal prosecutors throughout the US who specialise in cyberinvestigations and assist it in executing requests.

2.3.3 Conclusion

While there is still much more work to be done, States seem to be trying seriously to increase technological familiarity among those who handle mutual legal assistance requests.

2.4 Rec 4 – Training for MLA

> Parties should consider providing for better training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be supported by the capacity building programmes of the Council of Europe and other organisations.

2.4.1 Overview of follow up given

Because of the ever-increasing volume of international requests for electronic evidence, Parties recommended more specialised training, taught to more and more officials. Parties believed that this would speed up MLA and make the process more efficient.

Parties seem to take this recommendation seriously and try to implement it in many variations.[11]

Many States have training academies for police, prosecutors, and judges. Within these established academies, some have instituted or are developing regular or occasional training on:

- both general cyberknowledge and MLA requests involving electronic data (Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Denmark, Italy, Japan, Latvia, Lithuania, Moldova, Romania, Serbia, Slovakia, Switzerland, United States);
- MLA requests involving electronic data (Albania, Estonia, Portugal);
- general cyberknowledge (France, Montenegro, Netherlands, Norway).

While a course in general cyberknowledge is not the same as a course in MLA requests involving electronic data, any increase in technological knowledge will aid in processing such requests.

Other States provide training on one or both topics through channels other than an established academy (Australia, Austria, Canada, Hungary, Mauritius, Slovenia, Spain).

Some express interest in receiving training or are considering or planning it themselves (Dominican Republic, Finland, Poland).

Data under the jurisdiction of US law is the main target of many MLA requests. For this reason, various US agencies, including the Central Authority, the Federal Bureau of Investigation, and the Department of Justice's Computer Crime and Intellectual Property Section, provide as much training as possible to foreign partners on obtaining electronic evidence from the US. This training may be held in or outside the US or via video conference. Participants include judges, prosecutors, and police. In addition, the US takes part in the training of GLACY, the Organization of American States, the UN Office on Drugs and Crime, and other organisations.

Other States also note that their training focuses in part on obtaining data under US jurisdiction.

Many indicate that they participate in training provided by multilateral organisations, including the Council of Europe.

[11] Cyprus, Georgia, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine, and the United Kingdom did not reply to this question.

2.4.2 Examples of good practices

Belgium: a basic and an advanced cybercrime course are given each year and include MLA training. Trainee magistrates must take a three-day course on international police and judicial cooperation which covers cooperation in cybercrime/electronic evidence matters. Other magistrates may also take this course.

Czech Republic: the Judicial Academy regularly organises training. Every year there is a national training seminar on MLA for all prosecutors and judges. There is a meeting of specialists in MLA twice a year for prosecutors and once a year for judges. The regular academy training for judges and prosecutors includes seminars focused on cybercrime, economic crime, and other crimes. These seminars also usually cover MLA requests specific to such cases. Police training is also regular and a plan is in place to intensify and extend it. The aim is to standardise knowledge and practice in the detection and investigation of cybercrime and to share best practices. A current regular police course grants a certificate in forensic examination for those who pass the graduation test.

Denmark: the Police College is responsible for the professional development of the police, as the Director of Public Prosecutions is for prosecutors. The National Cyber Crime Center (NC3) has a central role in providing cybercrime training for both groups. Cooperation among these three entities and representatives from police districts led to a "National Cybercrime Programme, Level 1" in 2015 and a subsequent Level 2 programme. NC3 specialists receive training themselves, first via a mandatory three-week introductory programme and later via mandatory advanced training. National specialists and police who have completed the prerequisites may take courses from the European Cybercrime Training and Education Group, the European Union Agency for Law Enforcement Training, or the master's programme at University College Dublin. Officials are also offered internal technical courses as well as external courses, seminars, etc.

Lithuania: training and professional development is part of Lithuanian cybersecurity policy. Lithuania is an active participant in training conducted by EU agencies and other States, such as the UK and the US. Police officers take part in such training annually. The Criminal Police Bureau launched specialised training on various aspects of cybercrime investigation, including MLA, in 2014, targeting future staff of the specialised cybercrime units in ten county police headquarters. Up to four times a year, public prosecutors' offices across the country provide cybercrime-related training for specialised law enforcement and judicial authorities. The Prosecutor General's Office and the Criminal Police Bureau should shortly issue recommendations on cybercrime for public prosecutors that will cover legal qualifications, international cooperation, investigative techniques, and related topics.

Portugal: international cooperation is a regular topic for initial and subsequent training of judges and prosecutors at the Centre of Judiciary Studies. Modules on international cooperation are included in the initial programme, and seminars, conferences, and workshops on various international cooperation topics are available thereafter. Judges and prosecutors have a legal obligation to attend at least two training sessions per year and some take part in events on international cooperation.

Romania and Slovakia: both conduct, institutionalise, and participate in extremely extensive, diverse training programmes, conferences and other events for police, prosecutors, and judges. These events cover cybercrime, international cooperation, and obtaining evidence under US jurisdiction. Programmes are sponsored by national authorities, including the judicial academy, and by many international organisations, partner States, and academic organisations.

Spain: The initial training course for prosecutors includes two specific units, on MLA and one on cybercrime. Furthermore, each of the specialised Public Prosecutor's Office units holds at least one

meeting per year to update the training of prosecutors serving at those units. There are also common training sessions for both specialised units, including a specific training on Budapest Convention MLA tools. In addition, there are training activities on both topics open to all prosecutors who wish to participate. There is a very fluent collaboration of specialised prosecutors and judges in police training activities. Conversely, police experts provide training to prosecutors and judges. The INCIBE, the National Institute of Cyber Security, with the support of other entities, including the Organization of American States, organises courses on cybercrime and cybersecurity involving police officers and legal practitioners from Spain and Latin-American countries.

The Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania is supporting Parties and Observer States through a range of projects and activities in the implementation of the Budapest Convention, including in the follow up to this and other recommendations of the T-CY Report on MLA. These activities are not specifically referred to under each Recommendation. The relevant projects are listed in the appendix to this report.

2.4.3 Conclusion

States are placing increasing emphasis on training all the categories of officials who are involved in electronic evidence collection and exchange. As States continue their efforts, they could focus on how often training takes place, whether it is offered to enough domestic officials and to the correct people, and whether training is routine and mandatory or optional. In short, States should consider a systematic approach to training.

2.5 Rec 5 – 24/7 Points of contact

Parties and the Council of Europe should work toward strengthening the role of 24/7 points of contact in line with Article 35 Budapest Convention, including through:

a. Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities
b. Encouraging contact points to pro-actively promote their role among domestic and foreign counterpart authorities;
c. Conducting regular meetings and training of the 24/7 network among the Parties;
d. Encouraging competent authorities and 24/7 points of contact to consider procedures to follow up to and provide feedback to the requesting State on Article 31 requests;
e. Considering to establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests;
f. Facilitating 24/7 points of contact to play a supportive role in "Article 31" requests.

2.5.1 Overview of follow up given

The aim of this Recommendation was to encourage practical actions that are mostly within the power of States to carry out themselves.

Almost all States take actions to follow the Recommendation,[12] and almost all report that they ensure that trained and equipped officials are available to facilitate the operative work and conduct or support MLA requests involving electronic data.

Many encourage their contact points to promote their role among domestic and/or foreign counterparts (Belgium, Bulgaria, Croatia, Denmark, Dominican Republic, France, Hungary, Italy, Japan, Lithuania, Malta, Mauritius, Moldova, Netherlands, Romania, Serbia, Slovakia, Spain, Switzerland, United States).

Some have their officials teach at or attend meetings and training relating to the 24/7 system either domestically or with foreign partners (Belgium, Croatia, Hungary, Italy, Latvia, Liechtenstein, Mauritius, Moldova, Romania, Spain, United States).

In a handful of States, the competent authorities and 24/7 points of contact work on or take part in procedures to follow up to and provide feedback to the requesting State on Article 31 requests (Hungary, Lithuania, Malta, Slovakia, Spain, United States).

A significant number have formally or effectively established contact points in prosecution offices (Albania, Belgium, France, Italy, Liechtenstein, Lithuania, Malta, Mauritius, Netherlands, Romania, Serbia, Spain, Switzerland, United States). Moldova and Poland are considering doing so.

Similarly, the 24/7 points of contact in a significant number of States facilitate or support the processing of Article 31 requests (Armenia, Australia, Bulgaria, Canada, Czech Republic, Denmark,

[12] Note It was sometimes difficult to discern, based on the relatively brief replies, which actions a country had taken or which category of the question they fit into.
Cyprus, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, Ukraine, and the United Kingdom did not reply to the question.

France, Liechtenstein, Lithuania, Malta, Mauritius, Romania, Serbia, Slovakia, Spain, Switzerland, Turkey, United States).

2.5.2 Examples of good practices

Bulgaria: the point of contact meets very frequently with different law enforcement bodies in Bulgaria to promote its role and capabilities. It is located within the cybercrime investigation unit of the General Directorate Combating Organized Crime to ensure that it has properly trained personnel and national responsibility and capabilities. Via a network of informal connections, it maintains good relationships with different governmental and nongovernmental organisations and the private sector.

France: the highly-trained police assigned to the 24/7 contact point are in France's agency specialising in investigation of electronic crime, which facilitates the exchange of practical experience. The 24/7 point of contact is in direct contact with the Central Authority to ensure the best handling of MLA requests involving electronic data. The point of contact advises its foreign counterparts of the elements for an MLA request and connects those counterparts with the Central Authority when necessary.
Lithuania: the 24/7 contact point is the specialised cybercrime unit of the Criminal Police Bureau and also serves as the point of contact with Europol, service providers, and public prosecutors' offices. It informs others about its activities in training events and meetings. It often assists requesting states, national police units, and prosecution authorities with Article 31 requests and other inquiries.

Romania: the contact point is the specialised cybercrime unit of the Romanian Prosecutor's Office (Directorate for Investigating Organized Crime and Terrorism - Service for Combating Cyber-criminality). By law this unit has the following duties: provides specialised assistance and information about legislation, orders immediate preservation of computer data, seizes objects containing computer data or information related to traffic data upon request of a competent foreign authority. Moreover, it carries out and facilitates the execution of letters rogatory in cybercrime cases. Within the Romanian National Police a secondary 24/7 point of contact is established to assist the existing one from the Prosecutor's Office, namely the Service for combating Cybercrime. The two points of contact from the Prosecutor`s Office and Police closely coordinate their activities

United States: the staff of the 24/7 contact point, the Computer Crime and Intellectual Property Section in the Department of Justice, specialises in cybercrime, intellectual property crime, electronic evidence, and international cooperation. The staff of the Central Authority is trained in MLA requests involving electronic data. CCIPS and the Central Authority work together constantly. These offices lead or take part in many training sessions each year for foreign and domestic colleagues and strongly encourage participation in the 24/7 network. In these events and others, the US seeks feedback about its MLA processes.

2.5.3 Conclusion

States take a wide variety of steps to improve the connections between the offices that process MLA requests involving electronic data. Those steps are detailed extensively in the compilation of the Parties' answers, which is available to all Parties. The T-CY recommends continued focus on improvement of the process. The Council of Europe – including through projects in coordination with the T-CY – should support the sharing of experience among 24/7 contact points. Close coordination with justice authorities should be ensured.

2.6 Rec 6 – Streamlining MLA procedures

> Parties should consider streamlining the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.

2.6.1 Overview of follow up given

In making this Recommendation, Parties indicated their belief that States could take domestic, internal action to simplify their mutual legal assistance procedures without waiting for such changes to be required by treaty. States might be able to identify internal steps that were unneeded, particularly in the digital age.

Most States reported that they had already streamlined procedures.[13] If they explained how they had carried out this streamlining, States usually mentioned processing MLA relating to electronic evidence requests quickly, permitting direct prosecutor-to-prosecutor or judge-to-judge contact, consultation (for example, with the requesting authority or the executing office), and/or using electronic communication methods (Australia, Czech Republic, Estonia, Hungary, Japan, Liechtenstein, Lithuania, Malta, Mauritius, Norway, Romania, Serbia, Slovakia, Slovenia, Spain).

Different procedures have been mentioned for European Union member States. When appropriate under the applicable treaty, incoming MLA requests are sent directly to the competent judicial authority.

Italy and the Netherlands are studying how to improve their systems and expect to introduce legislation to do so.

2.6.2 Examples of good practices

Austria: best practice information sorted by country is available on the intranet.

Azerbaijan: internal regulations were changed by the General Prosecutor's Office so that urgent and important requests are executed by prosecutors.

Belgium: formerly, authorisations for house searches and seizures were required twice in MLA requests – once prior to execution and once prior to transmission of evidence. This double authorisation has been abolished.

Czech Republic: if a treaty sets up direct contact points between prosecutors or judges, the prosecutors or judges involved are responsible for the case and communications, but two central judicial authorities for MLA are available as "help desks." Normally, the prosecutors' offices on the several subordinate levels communicate only with their immediately-superior office. However, in MLA matters, a prosecutor from any of the levels may directly contact the Central Authority.14 The Ministry of Justice has the same direct contact with all Czech judges.

Philippines: The DOJ-OOC drafted and proposed the adoption of the Procedure in Drafting Mutual Legal Assistance Requests for Cybercrime and Cyber-Related Cases which reduces the number of steps required for processing mutual legal assistance requests.

[13] Croatia, Cyprus, Finland, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to this question. Albania, Bulgaria, Israel, Portugal, and Switzerland reported that there were no recent developments.
[14] This mechanism applies when no direct contacts have been set up by treaty.

Spain: The Central Authority (Ministry of Justice) makes full use of electronic communication means. In order to obtain swift MLA, it is important to strengthen direct cooperation as established in the Budapest Convention for urgent cases. Sometimes, although MLA is requested by traditional means (using official channels) via the Central Authority, it is possible for the LEAs of the requesting and requested states to take steps in an unofficial way before the formal request is received. An example of such direct cooperation was the handling of US MLA requests regarding cyber-attacks directed against SONY.

United States: the Central Authority established a Cyber Unit to handle MLA relating to electronic evidence. When possible, this unit executes the requests itself without referring the request to federal prosecutors' offices elsewhere in the US. Cyber Unit attorneys are assigned to specific States and regions. For that reason, foreign partners have a known, continuing contact for requests and questions.

2.6.3 Conclusion

A few States listed concrete new steps taken. Nevertheless, the T-CY recommends that States continue to review the effectiveness of their systems and look for steps that could be eliminated, especially by considering what partner States have done.

2.7 Rec 7 – Use of all channels

> Parties should make use of all available channels for international cooperation. This may include formal mutual legal assistance, police-to-police cooperation and others.

2.7.1 Overview of follow up given

This Recommendation had two main foundations: first, that formal mutual legal assistance channels normally are too slow and that any other legally-proper method may be faster, and, second, that formal MLA channels (at least in some States) are becoming clogged by the greatly-increasing volume of electronic evidence requests. Any legally-proper transfer of evidence that takes place outside formal channels may not only be faster but may make way for the requests that must go only through formal channels.

Most States make use of all applicable channels, including the 24/7 channel, police-to-police channels, foreign liaison officers, Europol, diplomatic channels, Interpol, the International Association of Prosecutors, Eurojust, the European Judicial Network, other cooperation networks, and formal mutual legal assistance.[15] Some answers are qualified; States note that they may choose a different channel if exigent circumstances exist (Azerbaijan, Croatia, France, Montenegro).

Two States mentioned specifically that they make direct requests to US-based Internet service providers without involving US authorities, as permitted by US law (Bulgaria, Lithuania). However, other sources – ISP transparency reports, for example – indicate that States other than Bulgaria and Lithuania make direct requests to US ISPs. It was apparently an oversight that States omitted this from their answers (many States seemed to respond to Question 7 only as the requested, not the requesting, country).

2.7.2 Examples of good practices

Canada: Canada encourages the use of all available channels, including formal MLA, police to police cooperation, and cooperation between prosecuting authorities. Its Central Authority created a list for its foreign partners of the types of evidence that can be obtained without the need for formal MLA. In training foreign partners, Canada routinely highlights the assistance that may be available without MLA.

Israel: Israel established a "National Cyber Centre" within the Israeli Police Cyber Unit and a Cybercrime Department within the State Attorney's Office. These offices are active in facilitating requests in non-formal channels.

Italy: the judicial police facilitate police-to-police cooperation and handle mutual legal assistance requests. There is an effective communication protocol to harmonise and speed the practices of police and prosecuting offices.

2.7.3 Conclusion

Most States assert that they use all available channels to seek information and that they make available numerous channels for States seeking information from them. The T-CY recommends that informal channels be used (and, if necessary, developed) to the greatest extent permitted by the relevant law. This will speed assistance and should also reduce backlogs in formal channels.

[15] Cyprus, Finland, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine, and the United Kingdom did not respond to this question. Albania reported no recent developments.

2.8 Rec 8 – Emergency procedures

> Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.

2.8.1 Overview of follow up given

A few States have established formal emergency procedures; this recommendation sought to determine the procedures followed by other States.

A limited number of States provided substantive responses to this question.16 Most of them discuss only how they would receive and handle emergency requests, not whether they have special legal powers to procure evidence more quickly. Most States do not discuss life-or-death situations specifically.

Almost all answers recognise that emergencies connected to electronic evidence occur. Overwhelmingly, States state that, in an emergency, their officials would work harder, work more quickly, and alert their domestic colleagues that the case was urgent. This approach should not be underestimated and its results would be received gratefully. However, this approach is dependent on the diligence and concern of the officials involved rather than on an established, well-understood procedure.

No State has a fully-reliable emergency procedure that covers all categories of data, including content. US law permits emergency disclosures of subscriber, traffic and content data, but this provision is not mandatory. Internet service providers that are covered by US law have discretion to make such disclosures or to decline.

2.8.2 Examples of good practices

Several States report in general that they take note when an incoming request is labelled as urgent. Alternatively, they themselves may realise that a request is urgent even when the requester fails to say so. They will then deal with the request as quickly as possible (Armenia, Canada, Denmark, Estonia, Israel, Italy, Liechtenstein, Serbia, Turkey, US [if voluntary disclosure is inapplicable]).

Bulgaria: if the requesting party notes that a request is urgent, there are procedures under the Electronic Communications Act for expedited access to required data.

Latvia: by regulation, a case is presumed to be urgent when it involves preventing or disclosing a criminal offence, saving a person's life, protection of the State, or public safety. In such cases, several categories of subscriber data can be disclosed in three hours or less.

Switzerland: on a case by case basis, prosecuting authorities may avoid or postpone procedural elements or preconditions that may slow down the process.

[16] Croatia, Cyprus, Finland, Georgia, Hungary, Iceland, Japan, Lithuania, Luxembourg, Moldova, Netherlands, Panama, Portugal, Slovakia, Slovenia, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to this question. Albania, Australia, Austria, France, Mauritius, Montenegro, and Romania referred to previous responses or had no developments to report.

2.8.3 Conclusion

The number of cases in which lives or physical injuries are threatened, and in which foreign-stored electronic evidence is crucial, is increasing. There is no reason to expect that the number will decrease in the future. Perhaps because policymakers are unaware of officials' urgent attempts to assist each other in emergencies, States have developed few or no specific digital emergency procedures other than to rely on their officials to find a way. The T-CY recommends briefings by practitioners for policy makers on this subject and persistent domestic efforts to improve and formalise emergency mechanisms.

2.9 Rec 9 – Confirmation of receipt and action taken

Parties should confirm receipt of requests systematically and give, upon request, notice of action taken.

2.9.1 Overview of follow up given

This recommendation derives from Parties' reports that they frequently did not know if a mutual legal assistance request had been received, whether it was progressing, or where to direct questions. This was especially frustrating if a request was pending for months or years.

Most States report some form of automatic confirmation of mutual legal assistance requests. Either affirmatively or on request, they also notify requesting States about the substantive action taken on the request.[17]

- Several States (Australia, Estonia, Finland, Hungary, Italy, Liechtenstein, Malta, Norway, Serbia, Slovakia) automatically confirm receipt of an MLA request. They also affirmatively provide information about the action on the request and/or the contact information of the official handling the case.

- Others automatically confirm receipt but provide status or contact information only on request (Romania, Slovenia, United States).

- A large group provides confirmation of receipt on request (Armenia, Azerbaijan, Austria, Belgium, Bosnia and Herzegovina, Canada, Dominican Republic, Japan, Latvia, Moldova, Montenegro, Spain, Turkey). Some also provide status information on request.

Two States – Bulgaria and Switzerland – do not have confirmation procedures, though Bulgaria is working toward this goal.

In several Parties (Azerbaijan, France, Israel, Lithuania, Mauritius, Netherlands) the 24/7 points of contact confirm receipt of requests. Some provide updates regarding the actions taken either automatically or upon request. It is unclear whether these answers apply to mutual legal assistance request procedures or only to initial 24/7 requests.[18]

2.9.2 Examples of good practices

Australia: within 2-5 business days, the Central Authority confirms in writing (normally email) the receipt of incoming requests, providing a file reference for them. Once the request is assigned to a case officer within the Central Authority, s/he provides his/her direct contact details to the foreign requester to facilitate updates.

Hungary: confirmation of receipt of the request and information about the main steps in fulfilling it are always provided to the requesting country. When the request is forwarded to the relevant chief prosecutor's office, written notice (with contact details) is sent to the requesting party.

Liechtenstein: when the request is assigned to a judge, the requesting State is immediately sent a confirmation of receipt with a case number and the judge's contact information. The requesting State is informed of the disposition of the case and then provided either the requested evidence or the reasons for declining the request.

[17] Croatia, Cyprus, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to the question. Albania and Portugal reported no developments.
[18] For example, the 24/7 point of contact of France only confirms receipt of preservation requests.

2.9.3 Conclusion

The best practice is automatically to confirm receipt of requests and, as the case proceeds, automatically to provide the detailed, direct contact information of the official handling it and updates on its status. However, States may not have the resources to do this. Thus, the T-CY recommends that any entry point for mutual legal assistance requests – including the 24/7 contact point, if it receives not only 24/7 requests but MLA requests – automatically confirm receipt.

States provided a wide variety of answers, and they were occasionally unclear about how easy it would be to obtain contact and status information in practice. Thus, the T-CY emphasises that States should take any possible steps to oil the mechanism. A requested State must ensure that the requesting State knows where to direct any queries about the status of the case. Such queries may be handled by the Central Authority, a prosecutor's office, etc., but the system will not work if the requesting State does not know whom to contact. Finally, the relevant official in the requested State must promptly provide status information on request as the case proceeds.

2.10 Rec 10 – Opening of domestic investigations

> Parties may consider the opening of domestic investigation upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA.

2.10.1 Overview of follow up given

The primary point of this recommendation was that States should transfer information as easily as legally possible. The Budapest Convention supplies a legal basis for the transfer of spontaneous information in Article 26 because such information may help another State to pursue criminality. Similarly, evidence from a domestic investigation may assist another State's investigation.

Recommendation 10 asked a compound question and States often responded only to portions.[19]

- Numerous States could use spontaneous information that was transmitted to them (Armenia, Australia, Azerbaijan, Belgium, Canada, Czech Republic, Denmark, Latvia, Mauritius, Norway, Portugal, Romania, Serbia).

- A handful specifically report that they could transmit spontaneous information to other States (Croatia, Czech Republic, Liechtenstein, Romania, Switzerland, Turkey).

- Generally, States can consider opening, or must open, domestic investigations when a foreign State makes a request. Cases are opened only if domestic requirements are satisfied and opening a case seems appropriate (Albania, Armenia, Australia, Austria, Belgium, Bosnia and Herzegovina, Canada, Czech Republic, Denmark, Finland, France, Germany, Japan, Liechtenstein, Mauritius, Poland, Portugal, Romania, Serbia, Slovakia20, Spain, United States).

- A few States do not usually open domestic investigations based on foreign requests (Lithuania, Moldova, Montenegro). Lithuania noted that this did not restrict information-sharing or slow MLA because domestic investigations are not necessary to speed the process of obtaining evidence. Moldova has opened one such case involving electronic evidence.

2.10.2 Examples of good practice

Austria: domestic investigations are often opened on foreign request.

Denmark: the possibility [of opening a domestic case] is always considered by the authority competent to process a request for MLA.

Germany: There is close cooperation between the German 24/7 contact point (assigned to the Federal Police Office) and a specialized prosecution office for combating cybercrime. On the basis of the information and requests collected by the 24/7 contact point, the prosecution office is often able to start its own criminal investigations.

[19] Cyprus, Georgia, Iceland, Luxembourg, Panama, Sri Lanka, Ukraine, and the United Kingdom did not respond to this question. Bulgaria and Israel had no developments to report.
[20] In Portugal, the domestic case must be opened for domestic purposes, not to assist with international cooperation. Romania and Slovakia pointed out that information in an MLA request may be used only for limited purposes. For that reason, it may be necessary to obtain permission before such information is used to open a domestic case.

Norway: a domestic investigation may be opened if the substantive facts of the case connect to Norway. It is not necessary for a State to ask Norway to do this; Norwegian authorities can consider this option themselves.

Serbia: on request, a domestic investigation is opened and all relevant information gathered in that process is shared with foreign authorities.

2.10.3 Conclusion

Increasingly, investigations entailing electronic evidence involve more than one country. A case may have roots or victims in ten or twenty States and, as a practical matter, investigators in one country may be able radically to shorten the work of others if they share their data. From this survey, it is not clear how often the mechanisms of spontaneous information or opening a domestic case are used and therefore whether they facilitate assistance as much as they could.

The T-CY recommends that Parties share good practices on the use of Article 26 Budapest Convention regarding spontaneous information.

2.11 Rec 11 – Electronic transmissions

> Parties should make use of electronic transmission of requests in line with Article 25.3 Budapest Convention on expedited means of communication.

2.11.1 Overview of follow up given

This recommendation arises from the need to streamline the mutual legal assistance process in as many ways as possible.

Replies were divided. Respondents tended to state either 1) whether they send requests electronically or 2) permit other States to send them electronically. Few States answered about both sides of this equation.[21]

In numerous States, electronic transmission is permitted if the case is urgent; if the partner State requests it; or if an electronic request is followed by a paper version (Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czech Republic, Japan, Liechtenstein, Lithuania, Montenegro, Poland, Slovakia, Switzerland, US). Canada encourages submission of requests electronically.

Some stated that electronic communication was available or even routine but did not specify if it was used for both incoming and outgoing cases and in non-urgent cases (Albania, Armenia, Australia, Austria ("often used"), Estonia, Finland, France, Hungary, Malta, Netherlands, Norway, Romania, Spain).

2.11.2 Examples of good practices

Hungary: electronic communication channels – such as Europol SIENA, Interpol, or email – are preferred.

Malta: fax, email, and paper copy are used.

Netherlands: fax and email are common.

Norway: the current practice is to use email.

Serbia: incoming and outgoing requests are transmitted by email and are followed by paper submissions.

Spain: use of email and fax is common.

2.11.3 Conclusion

It is not clear why electronic submissions should not be permitted in every case, not merely in urgent cases (even if a paper submission is required thereafter). No country mentions poor electronic security as a reason to bar electronic submissions. States may simply have not become accustomed to submissions in electronic format. Or States may not realise that, as the volume of requests increases, reliance on paper alone will become impractical.

[21] Cyprus, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to this question.
Italy had no update.
In other cases, it was not obvious if the country was responding as to 24/7 requests or as to mutual legal assistance requests, so those responses are not summarised.

2.12 Rec 12 – Specific and complete requests

Parties should ensure that requests are specific and complete with all necessary information.

2.12.1 Overview of follow up given

Requested States frequently report that incoming requests for MLA omit crucial elements – everything from substantive facts to the requester's contact information – and that such omissions cause needless delay.

Most States assert that their States already ensure that requests are specific and complete (Albania, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Hungary, Japan, Latvia, Liechtenstein, Lithuania, Malta, Mauritius, Moldova, Montenegro, Netherlands, Philippines, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Switzerland, Turkey, United States).22

Several States note specifically that their Central Authorities review outgoing requests to ensure that they are adequate. The Central Authorities discuss the drafts with the domestic officials involved if the drafts need improvement before transmission (Australia, Czech Republic, France, Japan, Malta, Moldova, Romania, Serbia, Slovakia, Spain, Turkey, United States).

States also emphasise:

- training for the various categories of their officials who draft MLA requests (Belgium, Mauritius, Montenegro, Netherlands, Slovakia);
- templates, checklists, guides, or statutory requirements for requests (Australia, Belgium, Croatia, Czech Republic, Denmark, France, Latvia, Mauritius, Moldova, Netherlands, Serbia, Slovakia);
- consultation and liaison with the requested country (Canada, Estonia, France, Lithuania, Malta, United States).

2.12.2 Examples of good practices

Australia: the Central Authority uses a standard format for outgoing requests which includes the categories of information required by partners. The CA welcomes feedback from partners about specifics that should be included in Australia's requests.

France: the Central Authority and liaison magistrates posted outside France consult on and review MLA requests. France has also produced a guide specific to obtaining electronic data stored in the US.

Mauritius: requests must comply with formats from GLACY training and Mauritian statutory requirements.

Moldova: requests must include the specific elements listed in the criminal procedure code.

Montenegro: the national judicial and prosecutor training centre regularly conducts training for judges and prosecutors regarding MLA. In addition, at least once a year, the Ministry of Justice organises regional meetings with representatives of the ministries of justice and the judiciary of States with which it has bilateral agreements to increase the efficiency of MLA.

[22] Cyprus, Georgia, Germany, Iceland, Luxembourg, Panama, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not reply to this question. Bulgaria and Norway reported no updates.

Slovakia: Slovak prosecutors have had numerous training sessions about obtaining evidence from abroad, particularly from the US. There are prosecutors specialising in international cooperation at all levels of the system (district, regional, central), and the General Prosecutor's Office provides guidance to them. Some have been trained in conjunction with experts from the Cybercrime Unit of the Police Presidium. Training that focused on MLA requests for electronic evidence has also been conducted for judges and prosecutors by the Judicial Academy.

Council of Europe: the Octopus Community includes a tool for international cooperation, including a step-by-step guide for MLA requests for data.

2.12.3 Conclusion

In general, requesting States report that they pay significant attention to drafting MLA requests to ensure the adequacy of outgoing MLA requests. Despite these efforts, requested States still report that incoming requests are often deficient.

The tactics listed above to address deficient requests – Central Authority review, training, checklists, specialisation, consultations - should improve the drafting process in a relatively short time if they are pursued seriously.

While some problems with obtaining and providing electronic evidence through MLA are difficult to fix, better drafting of requests and responses should be achievable and render the process more efficient.

2.13 Rec 13 – Flexible application of dual criminality standards

Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are reminded to apply the dual criminality standard in a flexible manner that will facilitate the granting of assistance.

2.13.1 Overview of follow up given

Electronic evidence is important now in the investigation of a variety of crimes in which international assistance would have been unnecessary in an earlier time. This Recommendation urges that legal bases for the transmission of evidence are interpreted to provide as much assistance as possible.

Overwhelmingly, States evaluate dual criminality not based on the label or strict elements listed in an MLA request, but on the conduct underlying the alleged crime (Albania, Armenia, Australia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Canada, Croatia, Czech Republic, Estonia, Finland, France, Japan, Liechtenstein, Lithuania, Malta, Mauritius, Poland, Portugal, Romania, Serbia, Spain, Switzerland, United States).[23]

Several States have not had any cases in which dual criminality has been the basis for refusing assistance or, while they have not seen the issue to date, they expect to handle relevant cases flexibly (Albania, Italy, Montenegro, Slovakia).

For other States, dual criminality is a requirement when coercive measures, such as search and seizure or interception and recording of telecommunications, are requested (Belgium, Czech Republic, Denmark, Netherlands, Norway, Slovakia, Turkey).[24]

The Czech Republic reports that it intends to withdraw its reservation made when depositing the instrument of ratification in relation to the dual criminality requirement of Article 29.4 Budapest Convention for international preservation requests.

2.13.2 Examples of good practices

Canada: with few exceptions, Canada's laws do not require dual criminality. In the limited circumstances in which it is required, Canada applies a flexible conduct-based approach and does not require an exact match in Canadian law to the foreign offence.

Portugal: Portuguese authorities may provide cooperation, even without reciprocity, based on the nature of the facts or the need to combat certain serious forms of crime. They may also do so if the cooperation can contribute to improving the situation of the accused or his or her social reintegration or clarify facts related to a Portuguese citizen.

Serbia: the dual criminality standard is applied flexibly to facilitate the granting of assistance. If a criminal act referenced in the MLA request is not foreseen by the Serbian criminal code, Serbia tries, whenever possible, to apply the provisions of its code that have the elements and modus operandi that are most like the act described in the MLA request.

[23] Cyprus, Georgia, Germany, Iceland, Luxembourg, Panama, Slovenia, Sri Lanka, "the Former Yugoslav Republic of Macedonia", Ukraine, and the United Kingdom did not reply to the question. Bulgaria reported no updates.
[24] These States noted that, to find a way to assist, they may seek additional facts from the requesting country, offer assistance that is not barred by the requirement, and so on.

2.13.3 Conclusion

States report that they are trying their best to evaluate flexibly and to assist each other according to their domestic law and relevant international agreements. The TCY recommends that they continue to evaluate dual criminality based on the facts of the alleged crime instead of the label or strict elements listed in the MLA request.

2.14 Rec 14 – Prior consultation

> Parties are encouraged to consult with authorities of requested Party prior to sending requests, when necessary.

2.14.1 Overview of follow up given

The basis of this recommendation was Parties' report that deficient formal mutual legal assistance requests mortgaged the time of both requesting and requested States yet delayed or prevented the transfer of evidence. Parties emphasised that very-basic contacts (a phone call, an email) early in the process could cure mistakes or problems before time was spent on an insufficient formal request.

Overwhelmingly, Parties consult other States before sending formal mutual legal assistance requests. This prior consultation takes various forms, including emailed questions, transmission of draft requests for the requested party to critique, and questions to locally-stationed foreign liaisons. Some States normally consult beforehand only in sensitive or complex cases or when dealing with new partner States.[25]

A few States do not seem normally to consult before sending a request (Moldova, Turkey).[26]

2.14.2 Examples of good practices

Bulgaria: Bulgarian law enforcement actively consults with authorities of the requested party prior to sending requests whenever possible. For example, Bulgarian law enforcement cooperates with US authorities through US liaison officers stationed in Bulgaria and other specially-designated cybercrime contacts.

Czech Republic: Czech judicial and central authorities regularly consult with their most-frequent foreign partners. In complex cases, this consultation takes place in writing directly between responsible authorities, via networks of MLA specialists, or via bi- or multilateral coordination meetings.

France: France's central authority and liaison magistrates have a constructive dialogue with the authorities of the requested party. France emphasized that such informal contacts are to facilitate assistance and should not become a filter before a formal request is sent.

Lithuania: requested parties are usually consulted prior to transmission of requests, especially when Lithuania is working with a new partner state or when the request is sensitive or complex.

Serbia: when necessary, Serbia consults with the requested party beforehand to develop a complete request and ensure that all the necessary actions can be taken and all the evidence gathered.

Slovakia: often communicates with the US Department of Justice even before sending a preservation request. For instance, in cases of lesser-known providers, it asks the US about the correct address or the provider's capability to preserve data.

[25] Several States endorse the practice of prior consultation but do not say whether *they* consult other States. Rather, they encourage other States to consult them (Armenia, Australia, Switzerland).

[26] Croatia, Cyprus, Finland, Georgia, Iceland, Israel, Latvia, Luxembourg, Panama, Sri Lanka, "The former Yugoslav Republic of Macedonia", Ukraine, and the United Kingdom did not reply to this question.

2.14.3 Conclusion

Most Parties report that before they send a formal MLA document, they consult the requested State, when necessary, via one of several mechanisms. This result does not seem to be consistent with the complaints that led to the Recommendation. It may be that States have increased their use of prior consultation. In any case, more-frequent prior consultation will reduce mistakes, expense, delays, loss of evidence, and wasted work.

2.15 Rec 15 – Transparency regarding requirements, thresholds and grounds for refusal

> Parties should consider ensuring transparency regarding requirements for mutual assistance requests, and reasons for refusal, including thresholds for minor cases, on the websites of central authorities.

2.15.1 Overview of follow up given

People are increasingly used to obtaining basic information via websites. Thus, Parties suggested that it would be helpful if, to the greatest extent possible, requirements could be posted publicly for the benefit of requesting States. Training, consultation, liaison, and other mechanisms are useful, but they do not necessarily reach everyone who may draft an MLA request. A website may reach more officials more quickly.

Many States did not respond to the question's suggestion that they post basic MLA information on a website.[27] Instead, they cite or link to the statutes and treaties relevant to their States and/or note that case information, including reasons for refusing a request, is transmitted privately to the requesting State.

However, numerous States do post basic MLA information and/or links to relevant statutes and treaties on public or somewhat restricted websites (Australia, Belgium[28], Canada, Czech Republic, Italy,[29] Japan, Moldova, Poland, Serbia, Spain, Switzerland, Turkey). Others are considering posting MLA information (Czech Republic (information beyond what it already posts), Finland, Netherlands, Slovakia, United States). Where such information is only made available in national languages the usefulness for other Parties is limited.

2.15.2 Examples of good practices

Canada: the Central Authority maintains a comprehensive public website that provides substantive and procedural guidance to Canadian and foreign officials on making effective MLA requests. The website addresses how to request assistance in minor matters. Practical guides and templates are available on the site.

Japan: the website of the Ministry of Justice provides detailed explanations in English on MLA requirements, including the reasons for refusal of requests.

Moldova: all information on the requirements for MLA requests is provided on the website of the General Prosecutor's office. The information is currently posted only in Moldovan, but Moldova is considering translating and posting the information in English.

Turkey: the Central Authority provides general and explanatory MLA information on its website as well as access to the basic law of Turkish MLA practice.

2.15.3 Conclusion

It appears that some States are unable to host and maintain an MLA website. States that can host sites should post as much general, public information as possible. Posted information should include statutes, treaties, templates, guides, online tools, etc., but not information that is specific

[27] Croatia, Cyprus, Georgia, Germany, Hungary, Iceland, Luxembourg, Montenegro, Panama, Slovenia, Sri Lanka, "The Former Yugoslav Republic of Macedonia", Ukraine and the United Kingdom did not respond to the question. Bulgaria and Israel reported no updates.
[28] Belgium posts this information on the website of the PC-OC.
[29] Italy uses the European Judicial Network site, which is not open to all Budapest Parties.

to a case. Such publication of MLA procedures would reduce work for officials at all stages of the MLA process and in both the requesting and requested States.

3 Time periods for data preservation (Rec 16)

The T-CY should facilitate greater transparency regarding the time period for data preservation upon a foreign preservation request in line with Article 29 Budapest Convention. The T-CY should document time periods.

3.1 Time periods

The following table represents the time periods for data preservation and for the extension of the period of preservation, as communicated by States:

Party	Time periods for preservation of data following a foreign request	Conditions and periods to extend or renew the preservation of specified data
Albania	90 days	90 days
Andorra	No information provided	No information provided
Armenia	No specific time limits	No information provided
Australia	Division 3 of Part 3-1A of the Telecommunications (Interception and Access) Act 1979 specifies that a carrier must preserve communications held on the day a foreign preservation notice is served until they receive notice from the Australian Federal Police that the preservation notice has been revoked. The Australian Federal Police must revoke a preservation notice if a foreign country did not make a request to the Attorney-General for data for a period of 180 days.	No mechanism exists to extend or renew the preservation of specified data. The requesting country needs to complete a new preservation request. The effective preservation period of 180 days exceeds the minimum 60 days stipulated in Article 29.
Austria	Preservation of data is not limited by any time limit.	An extension or renewal is possible subject to the receipt of a request of the requesting state and the proportionality of the continued preservation. Time limits or periods are not foreseen.
Azerbaijan	No information provided	No information provided
Belgium	No information provided	No information provided
Bosnia and Herzegovina	To settle this matter, it is necessary to harmonize the Rulebook on Keeping Archived Files and Documents in a way that all files are kept during the period prescribed by the Convention. The only exception would concern the existing electronic databases of the Central Authority that would be permanently kept.	To settle this matter, it is necessary to harmonize the Rulebook on Keeping Archived Files and Documents in a way that all files are kept during the period prescribed by the Convention. The only exception would concern the existing electronic databases of the Central Authority that would be permanently kept
Bulgaria	3 months	No extension permitted
Canada	Under the Protecting Canadians from Online Crime Act, Canada has the ability to preserve computer data on police demand or by court order. Usually, the	No extension permitted

Party	Time periods for preservation of data following a foreign request	Conditions and periods to extend or renew the preservation of specified data
	first step for the preservation of data under the Act is for Canadian police to make a preservation demand on the record holder. The legal threshold for making a preservation demand is that there must be reasonable grounds to suspect that: An offence has been or will be committed under a law for a foreign state; An investigation is being conducted by a person or authority with responsibility in that state for the investigation of such offences; and, The computer data is in the person's possession or control and will assist in the investigation of the offence. Preservation demands are valid for 90 days and cannot be renewed. However, Canadian police then have the ability to obtain a preservation order from a Canadian court, as explained below.	
Croatia	No information provided	No information provided
Cyprus	No information provided	No information provided
Czech Republic	There is no time limit set in Czech domestic law for such data preservation in line with Article 29 Budapest Convention. However, the MLA request should be sent as soon as possible.	
Denmark	6 months	No extension permitted
Dominican Republic	The period of time concerning this issue is of ninety (90) days	Renewable anytime asked for the same amount of days.
Estonia	Data preservation can be done very quickly, if possible during one day.	For data preservation general powers are used. No further conditions or time periods have are provided by the legislation.
Finland	No information provided	No information provided
France	90 days	90 days
Georgia	No information provided	No information provided
Germany	If data is seized following a request for expedited preservation the data may be kept as long as reasonably required for the investigation and, if court proceedings are initiated, as long as required for establishing the evidence.	See left column.
Hungary	3 months	No information provided

Party	Time periods for preservation of data following a foreign request	Conditions and periods to extend or renew the preservation of specified data
Iceland	No information provided	No information provided
Israel	The Israeli Law enables preservation for a time period of six months, based on a decision of a magistrate judge.	An Israeli magistrate judge can extend the time period beyond six months, under conditions he will decide upon based on a specific request. In practice, the court will consider the intensity of the infringement of the suspect and third party's privacy, in contrast of the investigative interest.
Italy	90 days	6 months
Japan	60 days	In case of data preservation based on voluntary cooperation by ISPs, the preservation period may be more than 60 days.
Latvia	30 days	Up to 90 days
Liechtenstein	Preservation of data is not limited by any time limit.	Time limits or periods are not foreseen.
Lithuania	Based on the provisions of the Law on Electronic Communication, service providers in Lithuania are obliged to preserve the data for 6 months with the possibility for one renewal for additional 6 months.	No specific conditions need to be met to extend or renew the preservation. Additional request for renewal is sufficient.
Luxembourg	No information provided	No information provided
Malta	communications data relating to Internet Access and internet e-mail for a period of six months from the date of communication; communications data concerning fixed network telephony, mobile telephony and Internet telephony for a period of one year from the date of communication.	
Mauritius	Until such time as may reasonably be required for the investigation of an offence; Where prosecution is instituted, until the final determination of the case; or Until such time as the Judge in Chambers deems fit.	Conditions, extension and renewal will depend on the requirements as set out in section 11(3) of the CMCA above.
Moldova	1 month	Up to six months
Montenegro	No time limit provided by the law	
Netherlands	90 days	90 days
Norway	90 days. If data is preserved on	

Party	Time periods for preservation of data following a foreign request	Conditions and periods to extend or renew the preservation of specified data
	international request it is not necessary to renew it, as this will typically be extended by Norwegian authorities.	
Panama	No information provided	No information provided
Philippines	6 months.	A one (1) time request for extension of a six month period for preservation may be allowed under R.A. No. 10175.
Poland	If data is preserved on international request it is not necessary to renew it	
Portugal	3 months	Up to one year
Romania	60 days	30 days
Serbia	No legislation on data preservation	
Slovakia	90 days	90 days
Slovenia	No legislation on data preservation	
Spain	90 days	90 days
Sri Lanka		
Switzerland	90 days	Requests for preservation of data can be extend or renewed anytime within the deadline to present the formal MLA request.
"The Former Yugoslav Republic of Macedonia"	No information provided	No information provided
Turkey	Although Budapest Convention article 29/7, advise parties to preserve data at least for 60 days, there are no specified article on preservation requests and preserving period. However Law no: 6706 article 8/1-c, which titled as "foreign judicial request" regulates preserving evidence, which also include preserving data temporarily, for 40 days. If the request is received in 40 days, the period of preserving of the data maintains. Traffic data are also kept for a certain period within the scope of Law No. 5651. According to Article 5/3 of Law No. 5651, hosting service providers are obliged to keep the traffic data of the hosting services that they provide, for a period of time not less than one year and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data. According to Article 6/1-b of Law No.	

Party	Time periods for preservation of data following a foreign request	Conditions and periods to extend or renew the preservation of specified data
	5651, access providers are obliged to save the traffic data of the services that they provide, for a period of time not less than six months and not more than two years, which shall be designated by the regulations, and are also obliged to ensure the accuracy, integrity and confidentiality of these data.	
Ukraine	No information provided	No information provided
United Kingdom	No information provided	No information provided
United States of America	90 days	90 days

3.2 Overview of follow-up reported

The T-CY was aware that requesting States can be confronted with variations in the implementation of preservation. In addition, it is often difficult to perfect and process a mutual legal assistance request before preservation periods expire, especially if an investigation is continuing to develop or if practical reasons such as translation cause delay. This Recommendation focuses on whether requesting States can reasonably count on the availability of the data they seek.

States' answers to this question tended to divide into two categories: those that have specific time periods and requirements for renewal and those that have no specific limits, often because they have no written governing law.[30]

Time periods for preservation vary somewhat among States that have such limits, but the majority favour longer periods:

- Only a few States use 60 days or less (Japan, Latvia, Romania).
- Most choose 90 days (Albania, Bulgaria, Canada, France, Hungary, Italy, Netherlands, Portugal, Slovakia, Spain, United States) or 180 days (Australia, Denmark, Lithuania, Malta).

Some States have limits that vary according to the request of the prosecutor or foreign State or they have no specific limits (Armenia, Austria, Czech Republic, Estonia, Liechtenstein, Mauritius, Montenegro, Poland, Serbia, Slovenia, Switzerland). These States may be able to preserve indefinitely if it is appropriate.

Providers may choose to preserve data for periods that are longer than required by the relevant law.

Overwhelmingly, States permit renewal (even if, formally, they require a new request). Only Bulgaria and Japan reported that renewal is not permitted. States sometimes limit the total length of time for which data may be preserved, including renewals. Where such limits exist, they are almost always between six months and two years (Albania, Australia, Canada, France, Italy, Lithuania, Malta, Mauritius, Netherlands, Portugal, Spain, United States).

[30] Azerbaijan, Belgium, Croatia, Cyprus, the Dominican Republic, Finland, Georgia, Iceland, Luxembourg, Moldova, Panama, Sri Lanka, "The former Yugoslav Republic of Macedonia", Ukraine, and the United Kingdom did not respond to this question.

3.3 Conclusion

The goal of lengthy preservation periods is to save data while Parties make their subsequent MLA requests. It seems that this can be achieved either by generous time periods coupled with smooth renewals or by preservation without time limits. To avoid mistakes, Parties should check with foreign partners about their exact terms of preservation. It would also be helpful for Parties to make preservation information readily available.

4 Recommendations 17 and 18

4.1 Rec 17 – multi-language templates

> Rec 17 - The Council of Europe should – under capacity building projects – develop or link to standardised, multi-language templates for Article 31-requests.

4.1.1 Follow up given

Under the project Cybercrime@EAP II the Council of Europe developed in 2016 draft templates for preservation requests to be used for requests under Articles 29 and 30 Budapest Convention and for requests for stored computer data (subscriber information, traffic data, content data) under Article 31 Budapest Convention.

These templates were developed in activities with Eastern Partnership States (Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine) and with the support of experts from France, Germany, Portugal, "the former Yugoslav Republic of Macedonia" and UK.

The template for preservation requests was reportedly tested in practice by Georgia and Moldova. France has adapted and further developed the template for its use in practice.

The templates foresee limited flow text and primarily rely on boxes to be ticked. This should facilitate their conversion to multi-language templates.

For many years, Slovakia has used a form for expeditious data preservation requests under Article 29, especially vis-à-vis the US.

4.1.2 Conclusion

Good progress was made in the development of the templates.

It is recommended to have selected experts from among the T-CY to review the templates and subsequently share them with the T-CY and with 24/7 points of contact as well as MLA authorities for comments.

4.2 Rec 18 – Online resource

> Rec 18 - The Council of Europe should explore the possibility of establishing an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.

4.2.1 Follow up given

The Cybercrime Division of the Council of Europe (T-CY Secretariat and Cybercrime Programme Office, C-PROC) began to set up the Octopus Community in 2014, including a tool on international cooperation.

Progress was presented to T-CY 14 on 1-2 December 2015, where the T-CY decided to "welcome the establishment of the Octopus Cybercrime Community and to call on T-CY Members and Observers to contribute to the tools available on this platform".

In 2016, the Council of Europe Secretariat sought the necessary data from Parties to the Convention. The data received was uploaded. By April 2017, from among 54 Parties, 16 had provided complete information, 21 Parties provided partial or incomplete information and 17 had not contributed to the community.

Technical limitations hinder the further development of the tool into a more user-friendly application. These include, for example, content volume capacity, flexibility of the content management system which jeopardizes users experience, accessibility and security of the platform. The T-CY Secretariat is working on proposals for outsourcing the Octopus Community in order to overcome technical limitations and allow for the further evolution of the Community.

4.2.2 Conclusion

Much progress has been made in the establishment of the tool which – once fully operational – should add much value to international cooperation non-cybercrime and e-evidence.

Parties are invited to provide the T-CY Secretariat with the necessary data to complete the information concerning their respective authorities and procedures. Further efforts should be made to make available complete information on all Parties.

Given limited internal capacities to address technical limitations and to sustain the further development of the Octopus Community an outsourcing option should be pursued. Parties and donors should consider voluntary contributions to support the further evolution of the Octopus Community.

5 Conclusions, recommendations and follow up

5.1 Conclusions

- Mutual legal assistance is and will remain the primary means for obtaining electronic evidence for use in criminal proceedings. While additional solutions are being pursued to address situations where MLA is not feasible, States need to undertake the necessary efforts to render MLA more efficient in situations where MLA is feasible. Follow up to the recommendations adopted by the T-CY in December 2014 helps achieve this objective.

- The T-CY welcomes that 40 Parties and Observers provided substantive information on follow-up given to these Recommendations. The Committee takes note of the fact that in certain cases further amendments to the information provided would be useful in order to fully understand the legal and factual situation in countries. The T-CY regrets that some Parties did not respond.

- Information received shows that follow-up has been given by many States to many of the Recommendations. Good practices are available with respect to all Recommendations as inspiration to other States.

- Information received sometimes conveys a rather optimistic picture on the functioning of MLA. States underline that they pay significant attention to ensuring their outgoing MLA requests are complete and accurate, while they are concerned that this is not the case for incoming requests. This suggests that further efforts are needed by the T-CY to follow the functioning of MLA in practice.

- Many States report that they keep statistics for MLA on cybercrime and electronic evidence. It would be useful for States to share such data with the T-CY.

5.2 Recommendations

With respect to the Recommendations adopted by the T-CY, further follow up is recommended:

Rec 1 Parties should fully implement and apply the provisions of the Budapest Convention on Cybercrime, including preservation powers (follow up to T-CY Assessment Report 2012). [31]

Further follow up to be given:

- ► Parties should continue their efforts to fully implement all provisions of the Budapest Convention, including domestic provisions which impact international cooperation.
- ► Parties should remove impediments to the execution of Article 29 on international preservation requests – that is, in particular, the need for an MLA request – and otherwise improve their domestic implementation.
- ► Parties should undertake the necessary reforms to include in their national law written and specific preservation provisions as recommended by the T-CY in the assessment reports on expedited preservation.[32]

[31] Cyprus, Georgia, Iceland, Luxembourg, Panama, Sri Lanka, "the Former Yugoslav Republic of Macedonia," Ukraine, and the United Kingdom did not reply to this question.

[32] Assessment report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e722e
Assessment Report: Implementation of the preservation provisions of the Budapest Convention on Cybercrime : supplementary report
https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168044be2b

Rec 2 Parties should consider maintaining statistics or establish other mechanisms to monitor the efficiency of the mutual legal assistance process related to cybercrime and electronic evidence.

Further follow up to be given:

- ► Parties should share available statistics and case studies with the T-CY Secretariat to permit continued assessment by the T-CY on the functioning of MLA in relation to cybercrime and e-evidence. The T-CY should facilitate the sharing of good practices to encourage Parties to maintain statistics.

Rec 3 Parties should consider allocating more and more technology-literate staff for mutual legal assistance not only at central levels but also at the level of institutions responsible for executing requests (such as local prosecution offices).

Further follow up to be given:

- ► States should maintain and consider strengthening their efforts to allocate technology-literate staff for MLA, in order to ensure efficient proceedings at central and regional levels.

Rec 4 Parties should consider providing for better training to enhance mutual legal assistance, police-to-police and other forms of international cooperation on cybercrime and electronic evidence. Training and experience exchange should in particular target prosecutors and judges and encourage direct cooperation between judicial authorities. Such training should be supported by the capacity building programmes of the Council of Europe and other organisations.

Further follow up to be given:

- ► States should consider a systematic approach to training on MLA and other forms of international cooperation on cybercrime and e-evidence.
- ► The Council of Europe (T-CY Secretariat or C-PROC) should establish a list of trainers and institutions that can offer standardized and replicable training on international cooperation on cybercrime and electronic evidence.

Rec 5 Parties and the Council of Europe should work toward strengthening the role of 24/7 points of contact in line with Article 35 Budapest Convention, including through:

a. Ensuring, pursuant to article 35.3 Budapest Convention that trained and equipped personnel is available to facilitate the operative work and conduct or support mutual legal assistance (MLA) activities
b. Encouraging contact points to pro-actively promote their role among domestic and foreign counterpart authorities;
c. Conducting regular meetings and training of the 24/7 network among the Parties;
d. Encouraging competent authorities and 24/7 points of contact to consider procedures to follow up to and provide feedback to the requesting State on Article 31 requests;
e. Considering to establish, where feasible, contact points in prosecution offices to permit a more direct role in mutual legal assistance and a quicker response to requests;
f. Facilitating 24/7 points of contact to play a supportive role in “Article 31” requests.

Follow up to be given:

- ► States should take further steps to improve cooperation between 24/7 points of contact and MLA authorities.
- ► The T-CY to discuss practical cases involving 24/7 points of contact to address problems.

- ► The Council of Europe, in coordination with the T-CY, to organize further workshops or training events for 24/7 points of contact established under Article 35 to facilitate the functioning of the Network.

Rec 6 Parties should consider streamlining the procedures and reduce the number of steps required for mutual assistance requests at the domestic level. Parties should share good practices in this respect with the T-CY.

Follow up to be given:

- ► States should consider – based on the experience of other States – further measures to reduce steps required for MLA.

Rec 7 Parties should make use of all available channels for international cooperation. This may include formal mutual legal assistance, police-to-police cooperation and others.

Follow up to be given:

- ► States should consider further developing informal channels of cooperation in accordance with relevant law.

Rec 8 Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers.

Follow up to be given:

- ► States should make policy makers aware of increasing situations where emergency procedures would be required to permit urgent disclosure of electronic evidence. Capacity building projects of the Council of Europe should facilitate the raising of awareness of decision-makers.
- ► States should improve and formalise emergency procedures for the disclosure of electronic evidence.
- ► Provisions on emergency procedures requiring preventive measures – via MLA and via direct cooperation with providers – should be considered in the preparation of a Protocol to the Budapest Convention.

Rec 9 Parties should confirm receipt of requests systematically and give, upon request, notice of action taken.

Follow up to be given:

► Entry points for MLA requests should automatically confirm receipt and provide detailed, direct contact information.

Rec 10 Parties may consider the opening of domestic investigations upon a foreign request or spontaneous information to facilitate the sharing of information or accelerate MLA.

Follow up to be given:

- ► States should provide further information on the application of this recommendation, including the use of spontaneous information (Article 26 Budapest Convention).

Rec 11 Parties should make use of electronic transmission of requests in line with Article 25.3 Budapest Convention on expedited means of communication.

Follow up to be given:

- ► States should remove undue obstacles preventing electronic transmissions.

Rec 12 Parties should ensure that requests are specific and complete with all necessary information.

Follow up to be given:

- States should share with the T-CY examples where difficulties are encountered due to inadequate MLA requests. This should help reconcile the views of States regarding outgoing versus incoming requests.

Rec 13 Pursuant to Article 25.5 Budapest Convention and Paragraph 259 Explanatory Report, Parties are reminded to apply the dual criminality standard in a flexible manner that will facilitate the granting of assistance.

Follow up to be given:

- States should continue to exercise flexibility in accordance with the Convention when applying the dual criminality standard.

Rec 14 Parties are encouraged to consult with authorities of requested Party prior to sending requests, when necessary.

Follow up to be given:

- States should make more frequent use of the option of prior consultation to reduce mistakes, delays and cost.

Rec 15 Parties should consider ensuring transparency regarding requirements for mutual assistance requests, and reasons for refusal, including thresholds for minor cases, on the websites of central authorities.

Follow up to be given:

- States should undertake further efforts to implement this Recommendation. They should also make use of the Octopus Community in this respect.

Rec 16 The T-CY should facilitate greater transparency regarding the time period for data preservation upon a foreign preservation request in line with Article 29 Budapest Convention. The T-CY should document time periods.

Follow up to be given:

- Parties should make time periods and other conditions for preservation more readily available on their MLA websites and at the Octopus Community.
- The T-CY considers that preservation periods of less than 90 days without the possibility of at least one renewal are not practical.

Rec 17 The Council of Europe should – under capacity building projects – develop or link to standardised, multi-language templates for Article 31-requests.

Follow up to be given:

- Selected experts from among T-CY members should review the templates drafted under capacity building projects and subsequently share them with the T-CY and with 24/7 points of contact and MLA authorities for comments and adoption.
- The templates should then be finalized and made available at the Octopus Community for use by Parties.

Rec 18 The Council of Europe should explore the possibility of establishing an online resource providing information on laws of Parties on electronic evidence and cybercrime as well as on legal thresholds, and evidentiary and other requirements to be met to obtain the disclosure of stored computer data for use in court proceedings.

Follow up to be given:

- Parties should complete the information on the online tool in international cooperation at the Octopus Community.
- The Council of Europe should consider outsourcing the Octopus Community to overcome technical limitations and sustain the further evolution of its tools. Parties and donors should consider voluntary contributions to support this.

5.3 Follow up

The sharing of cases, experience and issues regarding MLA and other forms of international cooperation should become a regular feature of T-CY plenaries.

Parties and Observers are invited to report back to the T-CY on follow up given during these sessions.

_____

6 Appendix: Follow up to T-CY MLA Recommendation through capacity building activities

The Cybercrime Programme Office of the Council of Europe (C-PROC) in Bucharest, Romania, became operational in April 2014 and is aimed to support countries worldwide in the implementation of the Budapest Convention, including follow up to recommendations of the T-CY.

By August 2017, the following projects were underway:

Project title	Region	Duration	Budget	Funding
Cybercrime@Octopus (number 3021)	Global	Jan 2014 – Dec 2019	EUR 3.5 million	Voluntary contributions (Estonia, Hungary, Japan, Monaco, Romania, Slovakia, UK, USA and Microsoft) [not yet fully funded]
Cybercrime@EAP II on international co-operation in the Eastern Partnership region (number 3271)	Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine	May 2015 – Dec 2017	EUR 800,000	EU/CoE joint project (Partnership for Good Governance)
Cybercrime@EAP III on public/private co-operation in the Eastern Partnership region (number 3608)	Armenia, Azerbaijan, Belarus, Georgia, Moldova, Ukraine	Dec 2015 – Dec 2017	EUR 1,200,000	EU/CoE JP (Partnership for Good Governance)
GLACY+ project on Global Action on Cybercrime Extended (number 3148)[33]	Global (hub or priority countries: Dominican Republic, Ghana, Mauritius, Morocco, Philippines, Senegal, Sri Lanka, Tonga	Mar 2016 – Feb 2020	EUR 10 million	EU/CoE JP
iPROCEEDS project targeting proceeds from crime on the Internet in South-eastern Europe and Turkey (3156)	Albania, Bosnia and Herzegovina, Kosovo[34], Montenegro, Serbia, "The former Yugoslav Republic of Macedonia", Turkey	Jan 2016 – June 2019	EUR 5.56 million	EU/CoE JP
CyberSouth on Cooperation on cybercrime in the Southern Neighbourhood Region (3692)	Algeria, Jordan, Lebanon, Morocco, Tunisia	July 2017 – June 2020	EUR 3.35 million	EU/CoE JP

[33] This project was preceded by GLACY (Global Action on Cybercrime from November 2013 to October 2016).
[34] *This designation is without prejudice to positions on status, and is in line with UNSC 1244 and the ICJ Opinion on the Kosovo Declaration of Independence.