African Forum on Cybercrime
Addis Ababa, 16 – 18 October 2018

The Budapest Convention 24/7 Points of Contact Network

Matteo Lucchetti
Programme Manager Cybercrime
Cybercrime Programme Office (C-PROC)
Council of Europe

matteo.lucchetti@coe.int

Cybercrime as a criminal justice matter – Main Challenges

- **Lack of common definition** of cybercrime amongst the criminal justice authorities
  - Importance of reliable statistics
- **Cybercrime legislation**
  - Definition of cybercrimes
  - Where was Crime Committed? Which Country has jurisdiction?
  - Need to adopt global standards, International Treaties
- Coping with **new technological paradigms – Capacity Building**
  - Cloud Computing, Darknet, virtual currencies, Internet of Things
  - Skills and competencies/ capacity building
  - Limited technical capabilities
- Legal grounds for effective **international cooperation**
  - Police to Police
  - International Judicial Cooperation
  - Interactions with international large service providers (Social Networks, etc.)

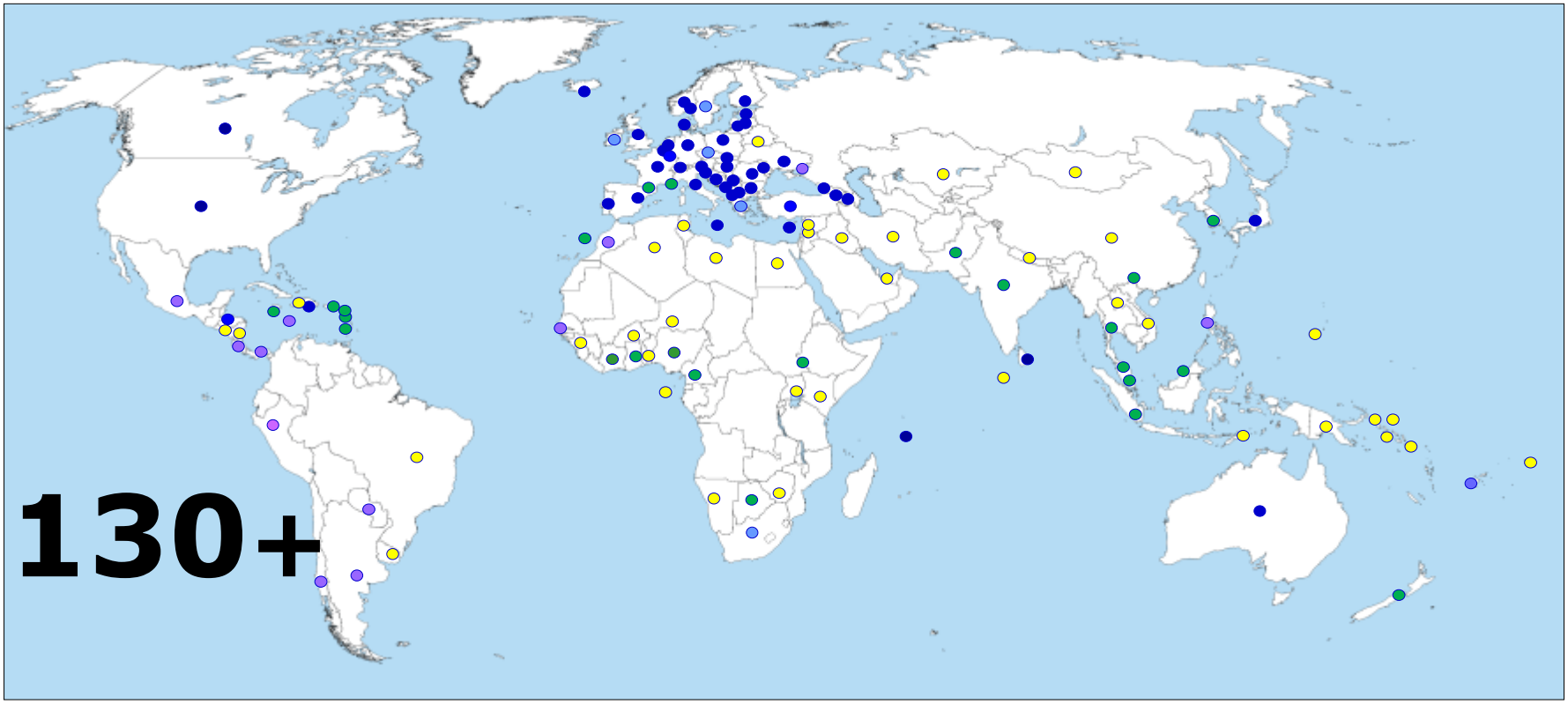
The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

2 Follow up and assessments: Cybercrime Convention Committee (T-CY)

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Reach of the Budapest Convention



Budapest Convention
Ratified/acceded: 61

Signed: 4

Invited to accede: 6
= 71

Other States with laws/draft laws largely in line with Budapest Convention = 20

Further States drawing on Budapest Convention for legislation = 45+

The Cybercrime Convention Committee (T-CY)

Established under Article 46 Budapest Convention

Membership (Sep 2018)**:**

- **61 Members** (State Parties)
- **14 Observer States**
- **12 organisations** (**African Union Commission**, Commonwealth Secretariat, ENISA, European Union, Eurojust, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Functions:

- **Assessments of the implementation of the Convention by the Parties**
- **Guidance Notes**
- **Draft legal instruments**

Two plenaries/year as well as Bureau and working group meetings

- **An effective follow up mechanism**
- **The T-CY appears to be the main inter-governmental body on cybercrime matters internationally**

Budapest Convention: scope

Criminalising conduct

- Illegal access
- Illegal interception
- Data interference
- System interference
- Misuse of devices
- Fraud and forgery
- Child pornography
- IPR-offences

+

Procedural tools

- Expedited preservation
- Search and seizure
- Production order
- Interception of computer data

+

International cooperation

- Extradition
- MLA
- Spontaneous information
- Expedited preservation
- MLA for accessing computer data
- MLA for interception
- **24/7 points of contact**

Harmonisation

24/7 Network (Art. 35)

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

Such assistance shall include **facilitating**, or, if permitted by its domestic law and practice, **directly carrying out** the following measures:

- the provision of technical advice;
- the **preservation of data pursuant to Articles 29 and 30**;
- the **collection of evidence**, the provision of legal information, and locating of suspects."

24/7 Network (Art. 35)

"A Party's point of contact shall have the **capacity to carry out communications with the point of contact of another Party on an expedited basis**.

If the point of contact designated by a Party is not part of that Party's authority or **authorities responsible for international mutual assistance or extradition**, the point of contact shall ensure that it is able **to co-ordinate with** such authority or authorities on an expedited basis.

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

Expedited preservation of data stored in a computer system – Art.29

- **Parallel framework to the internal provision**
  - allows one contracting Party to require from other Party the expedited preservation of data
  - if at the same time expresses its intention of sending a formal request of assistance for a search, or a seizure, or any similar measure

- The requested party must act as necessary, with all the due diligence, to preserve the requested data, according to its own national law

- Specificity of the digital environment - the necessity to **preserve something that, in very short moments, can be completely deleted**
- Only a preservation measure, for urgent reasons and **does not imply automatically disclosure of the preserved data** (non-intrusive)
- For **not less than 60 days (to enable request for S&S)**

Expedited disclosure of preserved traffic data – Art.30

- International equivalent of domestic power (Article 17)
- Where **pursuant to Article 29 request**, requested state observes that preserved traffic data reveals that **transmission of the communication was routed through a service provider** in
  - (i) a third state; or
  - (ii) the requesting state itself,
- it must **expeditiously disclose such preserved traffic data**
- Disclosure must be of **sufficient amount of data to identify service provider(s) involved and path of communication**
- Same grounds for refusal as before (political offence, prejudice to sovereignity, security, ordre public or other essential interest)

DATA PRESRVATION REQUEST under art. 29 and 30 BC – Template

Adopted by the T-CY at its 19th Plenary
Strasbourg, 9 July 2018

T-CY(2018)11

[Add logo or use letter head of requesting organization if necessary]

Data Preservation Request

under Articles 29 and 30 Budapest Convention on Cybercrime[1]

1 DATE
DD/MM/YYYY

2 REFERENCE / CASE NUMBER

3 REQUEST STATUS
☐ New request ☐ Extension of previous request ☐ Ticket/reference number of previous request:

4 REQUESTED AUTHORITY

5 REQUESTING AUTHORITY *	
Organisation	
Person in charge of the request	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	
Office Hours	
Time Zone	
☐	Response by email or other expedited means preferred
☐	Response preferred by means of:

[1] This template was adopted by the Cybercrime Convention Committee (T-CY) at its 19th Plenary (9-10 July 2018) to facilitate the preparation and acceptance of requests by Parties. Use of the template by Parties to the Budapest Convention is optional. Please note that items marked with asterisk (*) are required information pursuant to Article 29, paragraph 2 of the Convention on Cybercrime.

6 SHOULD ADDITIONAL CONFIRMATION FROM THE REQUESTING AUTHORITY BE NEEDED, PLEASE CONTACT:	
Name:	
Job Title:	
Function:	
Telephone number	
Cell phone number	
E-mail address	

7 INVESTIGATIVE/OPERATIONAL AUTHORITY IN CHARGE OF THE CASE (IF DIFFERENT FROM REQUESTING AUTHORITY)	
Organisation	
Person in charge at the authority	
Address	
Telephone number	
Cell phone number	
E-mail address	
Fax number	

8 PROSECUTION OFFICE OR COURT IN CHARGE IF APPLICABLE	
Prosecution office in charge and case number	
Court in charge and case number	
Prosecution or Court decisions related to the request	

9 FOLLOW UP THROUGH MUTUAL LEGAL ASSISTANCE	
☐	Please be informed that we intend to submit a request for mutual legal assistance to request the production of data.*
☐	Please find enclosed a mutual legal assistance request for the production of data.

10 OFFENCES SUBJECT TO CRIMINAL INVESTIGATION OR PROCEEDINGS*	
☐ Offence/s corresponding to Articles 2 through 11 Budapest Convention	Please specify offence under the law of the requesting State:
☐ Other offence/s	Please specify under the law of the requesting State:

2

DATA PRESRVATION REQUEST under art. 29 and 30 BC – Template

11 SUMMARY OF THE CASE*

Including:
- brief description of the facts
- how the data sought is related to the investigation/offences
- purpose and necessity of request for preservation and/or partial disclosure of traffic data
- charges pressed/list of offences in the case

12 DATA TO BE PRESERVED*

☐ **Subscriber information**	Please specify:	
Period of interest	Start date: DD/MM/YYYY Time (and time zone):	End date: DD/MM/YYY Time (and time zone):
☐ If the system is a shared system, please preserve all basic subscriber information for all virtual systems on the IP.		
☐ **Traffic data**	Please specify:	
Period of interest	Start date: DD/MM/YYYY Time (and time zone):	End date: DD/MM/YYYY Time (and time zone):
☐ **Content data**	Please specify:	
Period of interest	Start date: DD/MM/YYYY Time (and time zone):	End date: DD/MM/YYYY Time (and time zone):

13 INFORMATION IDENTIFYING THE PERSON OR ORGANISATION (E.G. SERVICE PROVIDER) IN POSSESSION OR CONTROL OF THE STORED COMPUTER DATA AND THE LOCATION OF THE COMPUTER SYSTEM, IF AVAILABLE*

14 EXPEDITED DISCLOSURE OF PRESERVED TRAFFIC DATA UNDER ARTICLE 30 OF THE CONVENTION ON CYBERCRIME

Details/description of data to be disclosed[3]

☐ This request seeks to preserve traffic data concerning a specific communication. If, in the context of this request, the server reveals that a service provider in another jurisdiction was involved in the transmission of this communication, please immediately disclose to us the identity of that service provider and the path of the communication in line with Article 30 of the Convention on Cybercrime.

[3] If necessary, please fill in the Annex (data specification form).

15 CASE STATUS

☐ Pre-trial phase
☐ On trial
☐ Crime in progress

Other details if necessary:

16 URGENCY

☐ **URGENT**
Response expected by: DD/MM/YYYY

REASONS FOR URGENCY

☐ Threat to life and limb
☐ Imminent threat of a serious nature to public security
☐ Crime in progress
☐ Suspect/offender in custody
☐ Suspect/offender about to be released from custody
☐ Volatility of data
☐ Statute of limitation due to expire
☐ Trial is imminent or in progress
☐ Other:

BRIEF DETAILS FOR URGENCY, IF ANY

17 CONFIDENTIALITY

☐ We request that that this preservation request is kept confidential and that customers are not notified.
Please inform us if your domestic law requires us to explain the reason for confidentiality; or – before taking any action – whether your domestic law requires customer notification or if you suspect that the provider may not comply with the request for confidentiality.

DATA PRESRVATION REQUEST under art. 29 and 30 BC – Template

18 CONFIRMATION / NOTIFICATION REQUESTED, IF AVAILABLE:
❑ Confirmation of receiving the request ❑ Confirmation of preservation of the data ❑ Information on the preservation period ❑ Information on whether data is beyond the jurisdiction of the requested country ❑ Information on whether the data preserved will be destroyed after the preservation period ❑ Other:

19 ADDITIONAL NOTES, IF ANY

20 SIGNATURE AND / OR STAMP OF REQUESTING AUTHORITY IF APPLICABLE	
Name	
Position	
Date / place	
Signature and/or stamp	

5

21 ANNEX: DATA SPECIFICATION FORM

Please complete a separate form for each person or organisation believed to be in possession or control of data. Please complete as much as is possible or applicable.

Details of person or organisation believed to be in possession or control of data		
Business Name		
Legal Name		
Contact name		
Address		
Country		
Phone		
Email		
Address		
IPv4	**1-255**	**1-255**
URL		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Port number		
IPv6	**Subnet – 64 bit**	**Host – 64 bit**
URL:		
Date		
Time		
Time Zone		
Proxy		
Anonymization		
Other data		
E-mail address		
Social Networking ID		
Date		
Time		
Time Zone		
Proxy		
Anonymization		

6

Mutual assistance regarding accessing of stored computer data – Art.31

- Request to another State to search or seize (and disclose) data stored by means of a computer system
  - Located within the territory of the requested State
  - Including data that has been preserved pursuant to Art. 29

- Enables a Party to **request another Party to undertake following measures** for benefit of the requesting party:
  - **Search or similarly access computer data**
  - **Seize or similarly secure computer data**

- Also **provides requested party with legal basis to disclose information** obtained as a result of exercise of such measures

The 24/7 POC Network: T-CY Recommendation

The T-CY completed an assessment of the functioning of mutual legal assistance under the Budapest Convention and adopted, inter alia, a **recommendation aimed at rendering 24/7 points of contact more effective**:

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;

The 24/7 POC Network: T-CY Recommendation

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.

Domestic responsibility supported by capacity building

The 24/7 POC Network

By April 2018, the Parties to the Budapest Convention had nominated 69 contact points, with 12 **Parties having established two different contact points**.

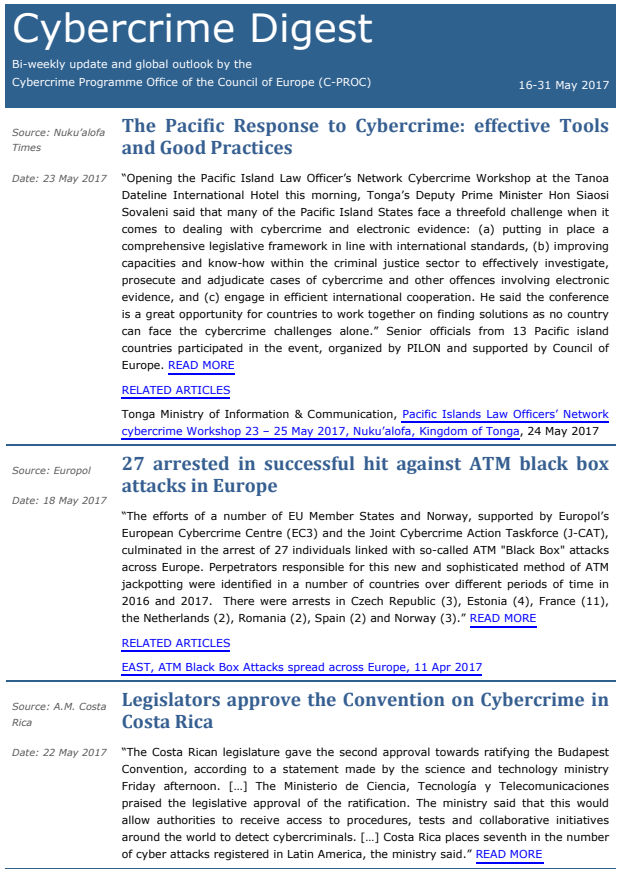
Since April 2018, 4 new countries have accessed the Budapest Convention, including Morocco.

Capacity building for 24/7 POC Network

- **Annual Meeting of the 24/7 POC Network – BC**
  - Started in 2017
- Targeted capacity building initiatives in countries supported by the **Capacity Building Programs of the Council of Europe**

Cybercrime@Octopus Community

- **Country Wiki**
- **Training Materials**
- **Cybercrime@CoE Update**
- **Cybercrime Digest**



Cybercrime Digest

Bi-weekly update and global outlook by the
Cybercrime Programme Office of the Council of Europe (C-PROC)

16-31 May 2017

Source: Nuku'alofa Times

Date: 23 May 2017

The Pacific Response to Cybercrime: effective Tools and Good Practices

"Opening the Pacific Island Law Officer's Network Cybercrime Workshop at the Tanoa Dateline International Hotel this morning, Tonga's Deputy Prime Minister Hon Siaosi Sovaleni said that many of the Pacific Island States face a threefold challenge when it comes to dealing with cybercrime and electronic evidence: (a) putting in place a comprehensive legislative framework in line with international standards, (b) improving capacities and know-how within the criminal justice sector to effectively investigate, prosecute and adjudicate cases of cybercrime and other offences involving electronic evidence, and (c) engage in efficient international cooperation. He said the conference is a great opportunity for countries to work together on finding solutions as no country can face the cybercrime challenges alone." Senior officials from 13 Pacific island countries participated in the event, organized by PILON and supported by Council of Europe. READ MORE

RELATED ARTICLES

Tonga Ministry of Information & Communication, Pacific Islands Law Officers' Network cybercrime Workshop 23 – 25 May 2017, Nuku'alofa, Kingdom of Tonga, 24 May 2017

Source: Europol

Date: 18 May 2017

27 arrested in successful hit against ATM black box attacks in Europe

"The efforts of a number of EU Member States and Norway, supported by Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT), culminated in the arrest of 27 individuals linked with so-called ATM "Black Box" attacks across Europe. Perpetrators responsible for this new and sophisticated method of ATM jackpotting were identified in a number of countries over different periods of time in 2016 and 2017. There were arrests in Czech Republic (3), Estonia (4), France (11), the Netherlands (2), Romania (2), Spain (2) and Norway (3)." READ MORE

RELATED ARTICLES

EAST, ATM Black Box Attacks spread across Europe, 11 Apr 2017

Source: A.M. Costa Rica

Date: 22 May 2017

Legislators approve the Convention on Cybercrime in Costa Rica

"The Costa Rican legislature gave the second approval towards ratifying the Budapest Convention, according to a statement made by the science and technology ministry Friday afternoon. […] The Ministerio de Ciencia, Tecnología y Telecomunicaciones praised the legislative approval of the ratification. The ministry said that this would allow authorities to receive access to procedures, tests and collaborative initiatives around the world to detect cybercriminals. […] Costa Rica places seventh in the number of cyber attacks registered in Latin America, the ministry said." READ MORE

- **Join the Octopus Community: https://www.coe.int/en/web/octopus/home**
- **Subscribe our Newsletters: https://www.coe.int/en/web/cybercrime/cyber-digests-and-updates**

Thank you

Matteo Lucchetti
Programme Manager Cybercrime
Cybercrime Programme Office (C-PROC)
Council of Europe

matteo.lucchetti@coe.int

Need to make MLA on cybercrime and e-evidence more efficient

- Implement provisions of Budapest Convention
- Statistics or other measures to monitor efficiency of the MLA process
- More technology-literate staff for MLA
- More training
- Strengthen 24/7 contact points
- Streamline procedures and reduce the number of steps required for MLA at domestic levels
- Make use of all available channels for international cooperation
- Establish emergency procedures
- Confirm receipts of MLA requests
- Open domestic investigations upon a foreign request or spontaneous information
- Electronic transmission of requests
- Make sure requests are specific and complete
- Consult foreign authorities before sending MLA requests

▸**Domestic responsibility supported by capacity building**

The accession process

1. **Expression of interest**
2. **Analysis of the legislation and of the context**
3. **Advisory mission on cybercrime legislation**
4. **Legislation in line with the provisions of the Budapest Convention**
5. **Request to join the BC, formalized by the Government and sent to the Council of Europe**
6. **Analysis of the request from the Treaty Office and decision from the Cybercrime Convention Committee**
7. **Invitation for the Country to join the BC**
8. **Ratification and instruments of accession deposited in Strasbourg**