

African Forum on Cybercrime

Addis Ababa, 16 – 18 October 2018



Global Action on Cybercrime

The GLACY+ Project

Matteo Lucchetti

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

matteo.lucchetti@coe.int

[**www.coe.int/cybercrime**](http://www.coe.int/cybercrime)



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 GFCE approach

The Delhi Communique

Theme 3. Cybercrime

- a) Enact and enforce a **comprehensive set of laws, guidelines, policies and programmes relating to cybercrime in line with existing international standards that allow for effective international cooperation**, such as the Budapest Convention on Cybercrime.
- b) Modernize and strengthen domestic criminal justice systems to deal with cybercrime and crimes involving electronic evidence [...]



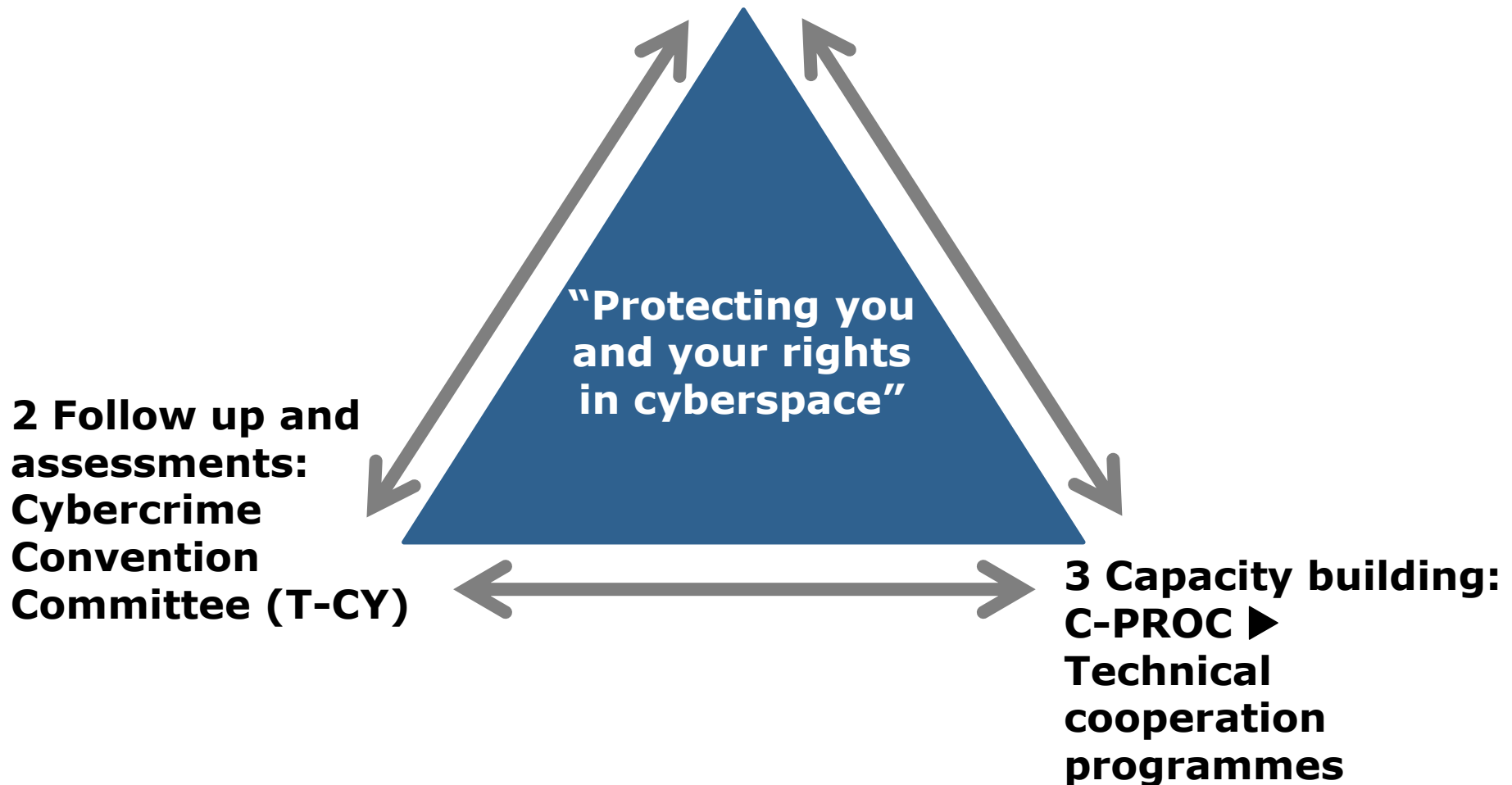
DELHI COMMUNIQUÉ ON A
GFCE GLOBAL AGENDA
FOR
CYBER CAPACITY BUILDING

24 November 2017



The approach of Council of Europe

1 Common standards: Budapest Convention on Cybercrime and relates standards

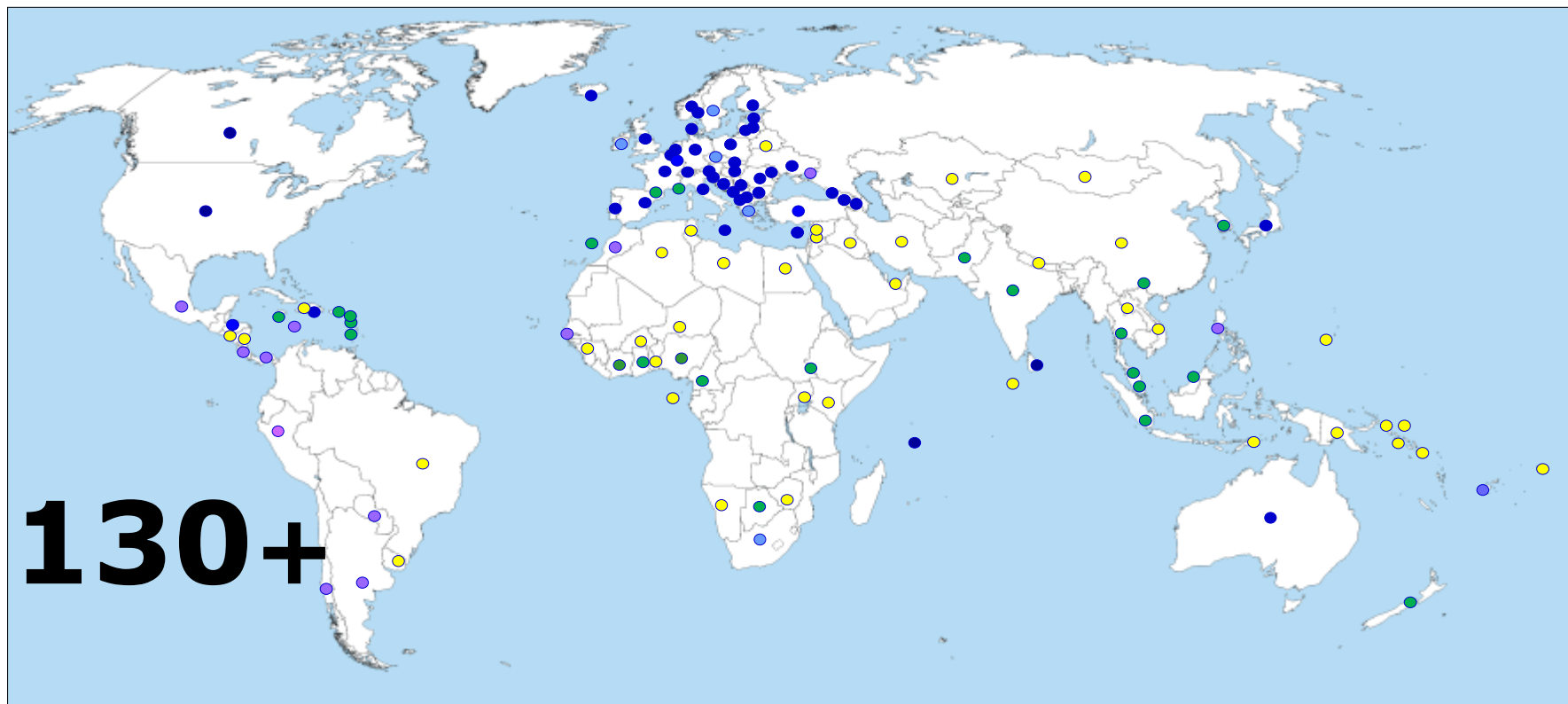




Council of Europe's Convention on Cybercrime – The Budapest Convention

- Opened for signature November 2001 in Budapest
- Followed by Cybercrime Convention Committee (T-CY)
- Open for accession by any State
- As of today, the only **international Treaty on cybercrime and electronic evidence**
- It gives high-level, technology-neutral definitions of cybercrime offences
- It sets standard procedures for investigation and prosecution on the national level, and puts relevant obligations on involved parties
- It defines procedural provisions for international cooperation, police-to-police and judicial
- It provides conditions and safeguards to meet the rule of law
- **Guidance notes** are published by T-CY to interpret BC provisions in the light of new threats and new technological paradigms

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+**



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





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**



Cybercrime Programme Office of the Council of Europe in Bucharest (C-PROC)

- **Committee of Ministers decision October 2013**
- **Operational as from April 2014**
- **Currently 26 staff**

- **Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence**

GLACY+

Global Action on Cybercrime Extended

GLACY+

EU/COE Joint Project on Global Action on Cybercrime Extended

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

To strengthen the capacities of States worldwide to apply legislation on cybercrime and electronic evidence and enhance their abilities for effective international cooperation in this area.

GLACY+ is intended **to extend the experience of the GLACY project**, which supports seven priority countries in Africa and the Asia-Pacific region. These **countries may serve as hubs to share their experience within their respective regions**. Moreover, countries of Latin America and the Caribbean may now also benefit from project support.

Duration	60 months (Mar 2016 – Feb 2021)		
Budget	EUR 13.5 million		
Funding	European Union (Instrument Contributing to Peace and Stability) and Council of Europe		
GLACY+ Priority and Hub countries	<ul style="list-style-type: none">• Cape Verde• Dom. Republic• Morocco• Senegal	<ul style="list-style-type: none">• Costa Rica• Ghana• Nigeria• Sri Lanka	<ul style="list-style-type: none">• Chile• Mauritius• Philippines• Tonga



GLACY+ Global Action on Cybercrime Extended

CYBERCRIME LEGISLATION, POLICIES AND STRATEGIES

- To promote consistent cybercrime legislation, policies and strategies as stand-alone and as part of broader cybersecurity

POLICE AUTHORITIES AND INVESTIGATIONS

- To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.

CRIMINAL JUSTICE AND INTERNATIONAL COOPERATION

- To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.



GLACY+ Objective 1

Cybercrime Policies and Strategies


Obj 1	To promote consistent cybercrime policies and strategies.
Result 1.1	Cybercrime policies and strategies as part of national cybersecurity frameworks strengthened in at least 16 countries (priority and a number of other countries) and experience shared with other countries.
Result 1.2	Policy dialogue and cooperation on cybercrime enhanced between international and regional organisations .
Result 1.3	Legislation on cybercrime and electronic evidence strengthened in line with the Budapest Convention and rule of law and human rights standards in priority countries and reforms have been initiated in additional countries.



GLACY+ Objective 2

Capacities of police authorities

Obj 2	To strengthen the capacity of police authorities to investigate cybercrime and engage in effective police-to-police cooperation with each other as well as with cybercrime units in Europe and other regions.
Result 2.1	Assessments/ cyber reviews (initial and final) of law enforcement capacities available for priority countries.
Result 2.2	Cybercrime and computer forensics units strengthened in priority countries and experience shared with other countries.
Result 2.3	Law enforcement training strategies available in priority countries, including access to ECTEG training materials.
Result 2.4	At least 500 LE officers trained in basic cybercrime investigations and computer forensics as well as related rule of law requirements.
Result 2.5	International police-to-police cooperation on cybercrime and electronic evidence is more effective.



GLACY+ Objective 3

Capacities of judicial authorities

Obj 3	To enable criminal justice authorities to apply legislation and prosecute and adjudicate cases of cybercrime and electronic evidence and engage in international cooperation.
Res 3.1	Assessments of criminal justice capabilities available for pri. countries
Res 3.2	Judicial training academies in at least ten countries are providing training on cybercrime and electronic evidence as part of their regular curricula and experience has been shared with other countries.
Res 3.3	Institutions strengthened and procedures improved for international judicial cooperation related to cybercrime and electronic evidence in at least 10 countries and experience shared with other countries.



Agreement AUC – COE for a collaboration in the area of cybercrime

Agreement for cooperation with the **African Union Commission to jointly assist African Countries in the strengthening of:**

- **their domestic legislation on the basis of the “Budapest Convention on Cybercrime” and the “African Union Convention on Cyberspace Security and Protection of Personal Data - Malabo Convention”;**
- **institutional capacities, training and international/regional cooperation;**
- **cybercrime policies and strategies.**

Through:

- Participation of CoE in **African Summits on topics related to cybercrime;**
- Joint organisation of an **awareness raising seminar on the Budapest Convention in Addis Ababa with the participation of Ambassadors to the African Union** in view of building synergies between the Budapest Convention and the Malabo Convention;
- Joint organization of an **“AFRICAN FORUM ON CYBERCRIME”** within the framework of the GLACY+ Project in 2018 aimed at promoting a coherent approach to capacity building on cybercrime and electronic evidence in Africa.

The African Forum on Cybercrime

Addis Ababa, 16-18 October 2018





Agreement ECOWAS – COE for a collaboration in the area of cybercrime

- Agreement for cooperation with the **ECOWAS Commission**
 - Regional/International meeting on **harmonisation of legislation** on Cybercrime and EE, rule of law and human rights safeguards with participation of all ECOWAS Member States
 - **Judicial training** on cybercrime and electronic evidence for all ECOWAS countries
 - Francophone and Lusophone countries in Senegal, March 2017
 - Anglophone countries in Ghana, December 2017



GLACY+ Activities in the African Region

- **East African Regional Conference on Cybercrime and Electronic Evidence**, in collaboration with the GPEN and with the participation of regional and international organizations and countries from East Africa (Mauritius)
- **Development of Cybercrime investigations, digital forensic capabilities** and workshop on interagency cooperation and PPP (Mauritius)
- **Workshop on data protection and INTERPOL Tools and Services** and support on how to set-up and strengthen the 24/7 POC (Senegal)
- **ECTEG Course**, Cybercrime and digital forensics specialized training for law enforcement officers (Ghana)
- **First responders Training of Trainers** (Senegal)
- **Advisory missions on cybercrime and cyber security policies and strategies** (Ghana, Mauritius, Senegal)
- **Judicial ToT on cybercrime and e-evidence** (Ghana, Mauritius, Senegal)
- **ToT for Judiciary Police** (Morocco)



GLACY+ Activities in the African Region

- **Meeting of the INTERPOL WG of the Heads of Cybercrime Unit of the African Region** (Mauritius)
- **Regional training for judges and prosecutors of the ECOWAS Region** (Francophone and Lusophone in Senegal, Anglophone in Ghana)
- **Advisory missions on legislation** (Mauritius, Burkina Faso, Uganda)
- **Support for the Technical Committee on Digital Rights and Freedom** (Nigeria)
- **Data Protection Bill** (Nigeria)
- **Streamlining MLA procedures on cybercrime and electronic evidence** (Mauritius, Senegal)
- In addition, several international events are organized/ supported, with participation of GLACY+ countries (e.g. **CyberDrill in Eastern Partnership Countries**, ICANN Capacity Building WS for African LEAs)

- **Capacity building backed up by common standards** (example: Budapest Convention) **and follow up mechanism** (example: Cybercrime Convention Committee of the Parties)
- **Political commitment to implement standards** (Example: signature or formal request for accession to Budapest Convention) as a prerequisite for full range of support
- **Rule of law conditions:** strengthening legislation, including safeguards for procedural powers, as starting point
- **Sequencing of activities:** Initial situation reports ► committing decision makers and counterpart organisations ► implementing activities ► assessing progress made ► feeding results back into policies
- **Country project teams** ► Example GLACY+: cooperation with 8 x 5 institutions
- **Capacities for capacity building** ► C-PROC

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

- **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>

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 Officers' 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](#)

African Forum on Cybercrime

Addis Ababa, 16 – 18 October 2018



Thank you

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

matteo.lucchetti@coe.int

[**www.coe.int/cybercrime**](http://www.coe.int/cybercrime)



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**