Regional workshop on

COVID-19 related cybercrime and e-evidence in Asia

Colombo, 7-9 March 2022

Session on enhanced cooperation and disclosure of electronic evidence

The Second Additional Protocol to the Convention on Cybercrime

Opening for signature: 12 May in Strasbourg!

Alexander Seger
Head of Cybercrime Division
Council of Europe

SRI LANKA CERT|CC

ICTA ideas actioned
Information and Communication Technology Agency

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

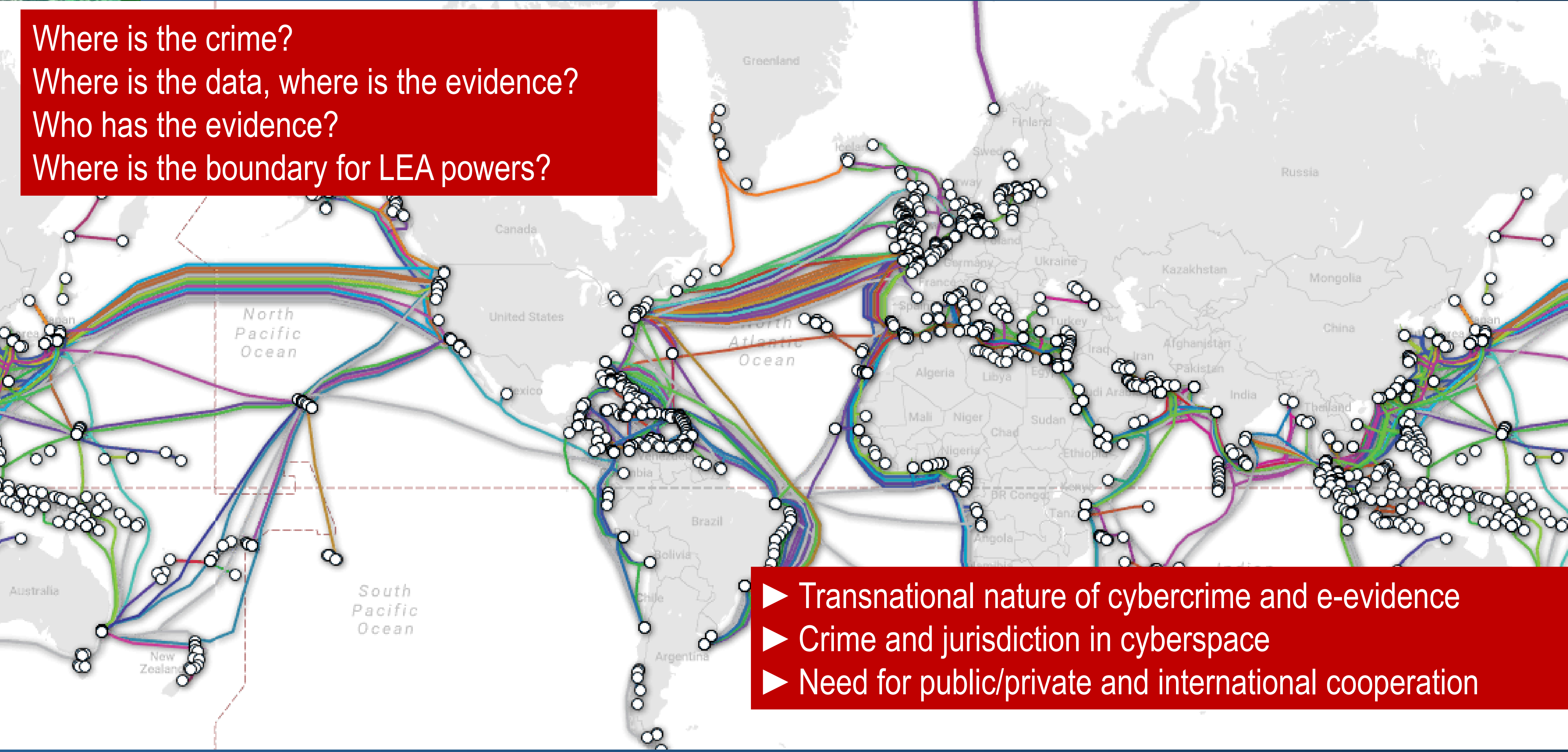
What crime?

Who did it?

What evidence?

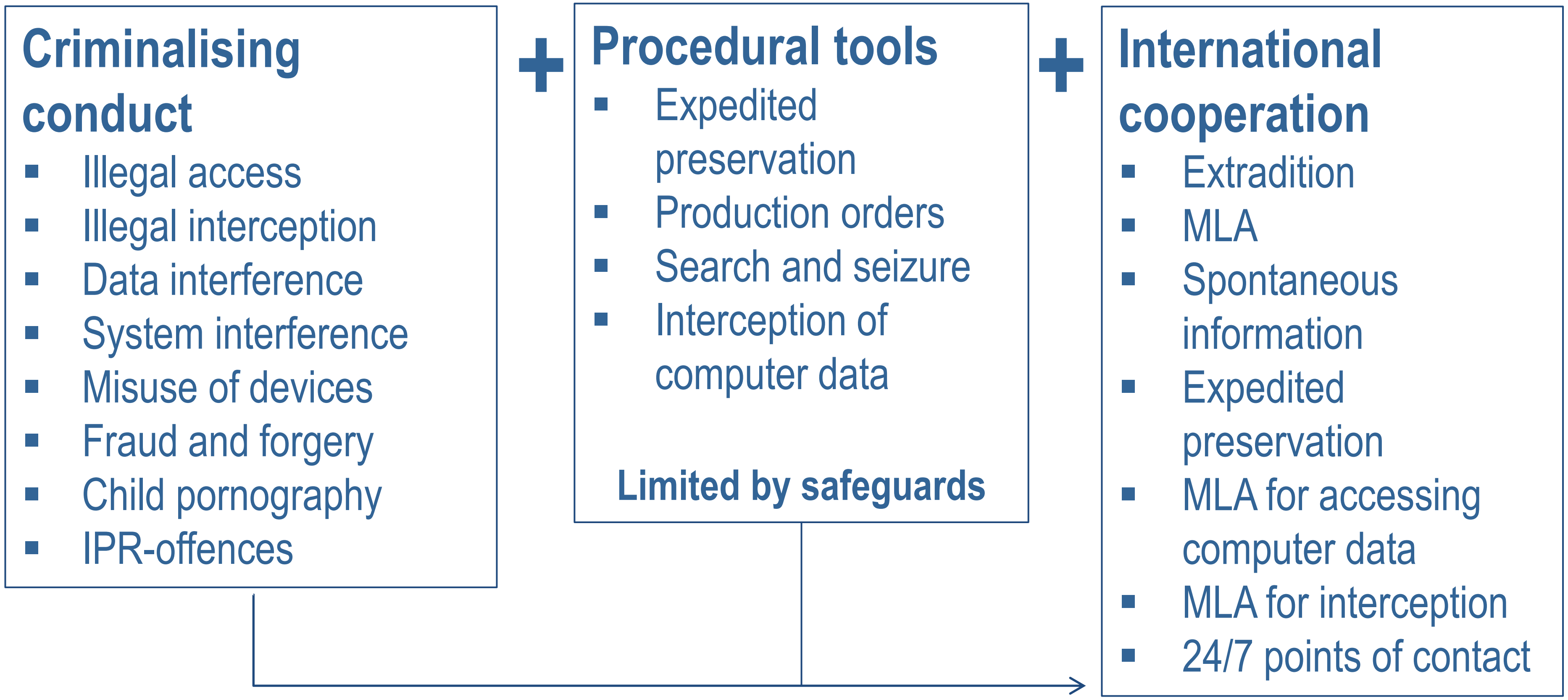
Cybercrime and e-evidence: the problem of territoriality and jurisdiction

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?



- ► Transnational nature of cybercrime and e-evidence
- ► Crime and jurisdiction in cyberspace
- ► Need for public/private and international cooperation

Content of the Budapest Convention



Criminalising conduct

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

Procedural tools

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

Limited by safeguards

International cooperation

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

Procedural powers and international cooperation for any criminal offence involving evidence on a computer system!

Example: Article 18 – Production order

Article 18 – Production order

1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit **subscriber information** relating to such services in that service provider's possession or control.

Guidance Note (2017) on Article 18 Budapest Convention on production of subscriber information:

- Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

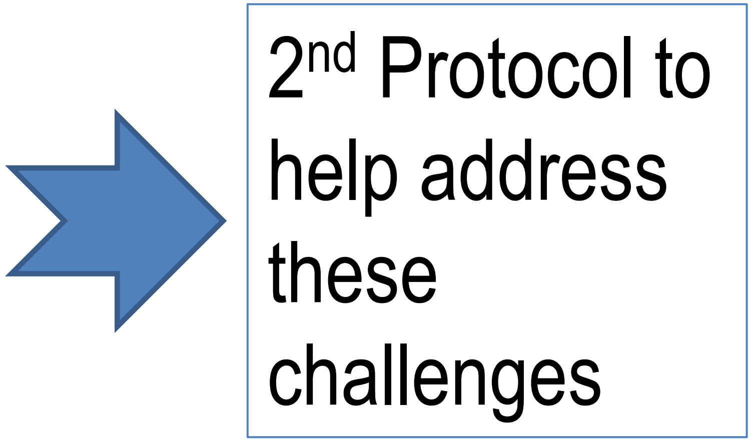
Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Territoriality and jurisdiction: Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- MLA and e-evidence
- Effective means not available to obtain the disclosure of e-evidence

► Less than 0.1% of offences in cyberspace lead to prosecutions and convictions

► Do victims obtain justice?



2nd Protocol to help address these challenges

Rationale: Why a 2nd Additional Protocol to the Budapest Convention?

- How to obtain subscriber information efficiently?
- How to cooperate directly with a service provider in another Party?
- How to obtain WHOIS data (domain name registration information) from registrars?
- How to obtain stored data, including content, in an emergency situation?
- How to make mutual assistance more effective?
- How to reconcile efficient and effective measures with rule of law and data protection requirements?

2nd Additional Protocol to the Convention on Cybercrime: the process of negotiations

Protocol:

- Prepared by Protocol Drafting Plenary and Drafting Groups established by the Cybercrime Convention Committee September 2017 to May 2021
- 91 sessions of the PDP, PDG and PDG subgroups
- 75 States and several international organisations participated with over 620 experts
- Data protection experts participated in negotiations
- 6 rounds of stakeholder consultations

= Carefully calibrated text designed to be consistent with the acquis of the Council of Europe but also to meet the requirements of all other Parties to the Budapest Convention

2nd Additional Protocol to the Convention on Cybercrime: the process of negotiations

✓ 28 May 2021 – Approval of the draft Protocol by Cybercrime Convention Committee

✓ 17 November 2021 – Formal adoption of Protocol by Committee of Ministers of the Council of Europe

Next:

► 12 May 2022, in Strasbourg, France – Opening for signature

2nd Additional Protocol to the Convention on Cybercrime: content

Preamble

Chapter I: Common provisions

Article 1 Purpose

Article 2 Scope of application

Article 3 Definitions

Article 4 Language

Chapter II: Measures for enhanced cooperation

Article 5 General principles applicable to Chapter II

Article 6 Request for domain name registration information

Article 7 Disclosure of subscriber information

Article 8 Giving effect to orders from another party for expedited production of subscriber information and traffic data

Article 9 Expedited disclosure of stored computer data in an emergency

Article 10 Emergency mutual assistance

Article 11 Video conferencing

Article 12 Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

Article 13 Conditions and safeguards

Article 14 Protection of personal data

Chapter IV: Final provisions

Article 15 Effects of this Protocol

Article 16 Signature and entry into force

Article 17 Federal clause

Article 18 Territorial application

Article 19 Reservations and declarations

Article 20 Status and withdrawal of reservations

Article 21 Amendments

Article 22 Settlement of disputes

Article 23 Consultations of the Parties and assessment of implementation

Article 24 Denunciation

Article 25 Notification

Example: Direct disclosure of subscriber information

Second Additional Protocol to the Budapest Convention on Cybercrime:

Article 7 – Direct disclosure of subscriber information

Direct disclosure of subscriber information: the issue

Cybercrime Convention Committee ▶ Cloud Evidence Group (2016)

- Subscriber information most often required in criminal investigations. Often starting point of an investigation.
- Less privacy-sensitive than traffic or content data. Rules for access to subscriber information not harmonised.
- Subscriber information held by service providers and obtained through production orders. Lesser interference in rights than search and seizure.

Field	Value
Login (account)	First.Last@xxxxxxx.com
First Name	First
Last Name	Last
State	Washington
Zip	98000
Country	USA
Time zone	UTC-8
Registered from	IP 65.55.161.10
Date Registered	10/24/2007 1:05:18 PM
Last Login	IP 64.4.1.11

Direct disclosure of subscriber information: the issue

Issue: Voluntary disclosure [of subscriber information] by service providers

Current practices:

- More than 200,000 requests/year by BC Parties/Observers to major US providers
- Disclosure of subscriber information (ca. 64%)
- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No disclosure by non-US providers
- No admissibility of data received in some States

► Clearer / more stable framework required

Direct disclosure of subscriber information: the issue

Example: Article 18 – Production order

Article 18 – Production order
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:

a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and

b a service provider offering its services in the territory of the Party to submit **subscriber information** relating to such services in that service provider's possession or control.

Guidance Note (2017) on Article 18 Budapest Convention on production of subscriber information:

- Domestic production orders for subscriber information if a provider is in the territory of a Party even if data is stored in another jurisdiction (Article 18.1.a)
- Domestic production orders for subscriber information if a provider is NOT necessarily in the territory of a Party but is offering a service in the territory of the Party (Article 18.1.b)

2nd Additional Protocol to the Convention on Cybercrime: content / example

Article 7 – Disclosure of subscriber information

1. Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to issue an order to be submitted directly to a service provider in the territory of another Party, in order to obtain the disclosure of specified, stored subscriber information in that service provider's possession or control, where the subscriber information is needed for the issuing Party's specific criminal investigations or proceedings.

2. a. Each Party shall adopt such legislative and other measures as may be necessary for a service provider in its territory to disclose subscriber information in response to an order under paragraph 1.

…..

Key elements:

- procedural power for competent authorities in a Party to issue an order to a service provider in another Party;
- an obligation for Parties to adopt any necessary measures for service providers in their territory to respond to an order issued by a competent authority in another Party;
- standard format (minimum information) to be provided by an authority issuing an order and additional information;
- notification or consultation procedure (discretion) – single authority (registry to be updated regularly);
- grounds for refusal;
- timeframe for execution;
- specific enforcement mechanism;
- electronic transmission;
- declaration;
- reservation.

Issue: Cooperation in an emergency

Article 3 – Definitions

…

2. For the purposes of this Protocol, the following additional definitions apply:

….

c. an “emergency” means a situation in which there is a significant and imminent risk to the life or safety of any natural person;

Examples:

Hostage situations, kidnappings, ongoing sexual abuse of a child, anticipated terrorist attack, cyber attacks on critical infrastructure resulting in imminent death or injury.

Articles

- ► 9 Expedited disclosure of stored computer data in an emergency
- ► 10 Emergency mutual assistance

2nd Additional Protocol to the Convention on Cybercrime: content / example

Article 9 – Expedited disclosure of stored computer data in an emergency

1. a. Each Party shall adopt such legislative and other measures as may be necessary, in an emergency, for its point of contact for the 24/7 Network referenced in Article 35 of the Convention ("point of contact") to transmit a request to and receive a request from a point of contact in another Party seeking immediate assistance in obtaining from a service provider in the territory of that Party the expedited disclosure of specified, stored computer data in that service provider's possession or control, without a request for mutual assistance.

   b. A Party may, at the time of signature of this Protocol or when depositing its instrument of ratification, acceptance or approval, declare that it will not execute requests under paragraph 1.a seeking only the disclosure of subscriber information.

2. Each Party shall adopt such legislative and other measures as may be necessary to enable, pursuant to paragraph 1:

   a. its authorities to seek data from a service provider in its territory following a request under paragraph 1;

   b. a service provider in its territory to disclose the requested data to its authorities in response to a request under paragraph 2.a; and

   c. its authorities to provide the requested data to the requesting Party.

……

2nd Additional Protocol to the Convention on Cybercrime: content / example

Article 10 – Emergency mutual assistance

1. Each Party may seek mutual assistance on a rapidly expedited basis where it is of the view that an emergency exists. A request under this article shall include, in addition to the other contents required, a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it.

2. A requested Party shall accept such a request in electronic form. It may require appropriate levels of security and authentication before accepting the request.

3. The requested Party may seek, on a rapidly expedited basis, supplemental information in order to evaluate the request. The requesting Party shall provide such supplemental information on a rapidly expedited basis.

4. Once satisfied that an emergency exists and the other requirements for mutual assistance have been satisfied, the requested Party shall respond to the request on a rapidly expedited basis.

5. Each Party shall ensure that a person from its central authority or other authorities responsible for responding to mutual assistance requests is available on a twenty-four hour, seven-day-a-week basis for the purpose of responding to a request under this article.
6. ……

2nd Additional Protocol to the Convention on Cybercrime: content / example

Issue: Efficiency versus safeguards

Means for a more effective criminal justice response:

- Direct cooperation with service providers in other jurisdictions to obtain subscriber information
- Direct requests to registrars to obtain domain name registration information
- More effective means to obtain subscriber information and traffic data through government-to-government cooperation
- Expeditious cooperation in emergency situations
- Joint investigations and video-conferencing

Subject to a particularly strong system of safeguards:

- Article 2 – scope of Protocol: specific criminal investigations or proceedings related to cybercrime and e-evidence
- Article 13 incorporates Article 15 of the Convention to ensure the adequate protection of human rights and liberties and that provides for the principle of proportionality
- Article 14 provides for detailed data protection safeguards that are unique for a criminal justice treaty
- Articles specify types of data to be disclosed
- Articles specify information to be included to permit application of domestic safeguards
- Reservations and declarations to permit domestic safeguards and limit information to be provided

2nd Additional Protocol to the Convention on Cybercrime: benefits

Benefits of the Protocol

Operational value:

- Legal basis for disclosure of WHOIS information
- Basis for direct cooperation with service providers for subscriber information (“direct disclosure”)
- Effective means to obtain subscriber information and traffic data (“giving effect”)
- Cooperation in emergencies (“expedited disclosure” + “emergency MLA”)
- Mutual assistance tools (“video-conferencing”, “JITs”)
- Data protection safeguards to permit the flow of personal data under the Protocol

Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

Conference on

enhanced cooperation and disclosure of electronic evidence

and

opening for signature of the 2nd Additional Protocol

Strasbourg, France, 12-13 May 2022

www.coe.int/cybercrime