International Law Association
Building tomorrow – Panels of the Committee on Digital Challenges for International Law
Online, 16 December 2021

Cybercrime, e-evidence and the rule of law in cyberspace:

How relevant is the criminal justice response?

Some hypotheses – and solutions

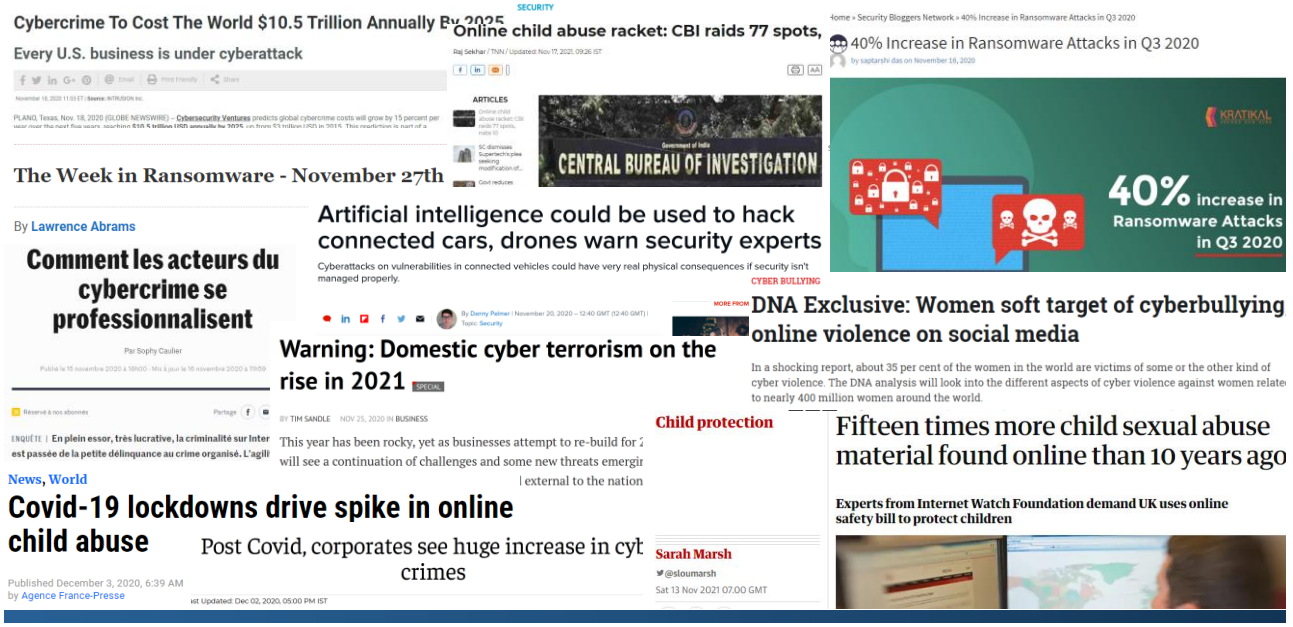
Alexander Seger
Head of Cybercrime Division
Council of Europe

BUDAPEST CONVENTION ON CYBERCRIME
OF THE COUNCIL OF EUROPE
CONVENTION DE BUDAPEST SUR LA CYBERCRIMINALITÉ
DU CONSEIL DE L'EUROPE
20 SINCE 2001
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

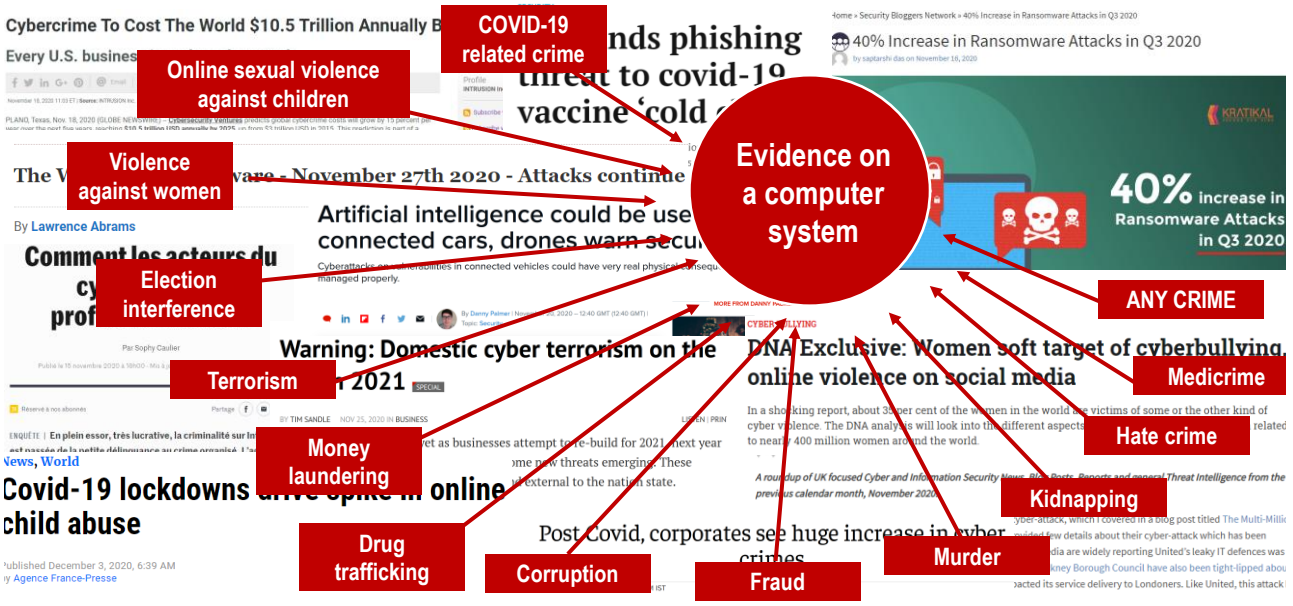
1

The problem of cybercrime …



2

… and e-evidence re all types of crime



3

Cybercrime and e-evidence as matters of criminal justice

- Hundreds of millions of incidents of theft of personal data every year
- Online child sexual abuse
- Cyberbullying, harassment and others forms of cyberviolence
- Massive fraud generating massive amounts of crime proceeds
- Attacks against critical information infrastructure
- Ransomware
- Interference in computer systems used in elections
- COVID-19 related crime online
- + other offences involving electronic evidence

Threats to

- Human rights
- Democracy
- Rule of law

4

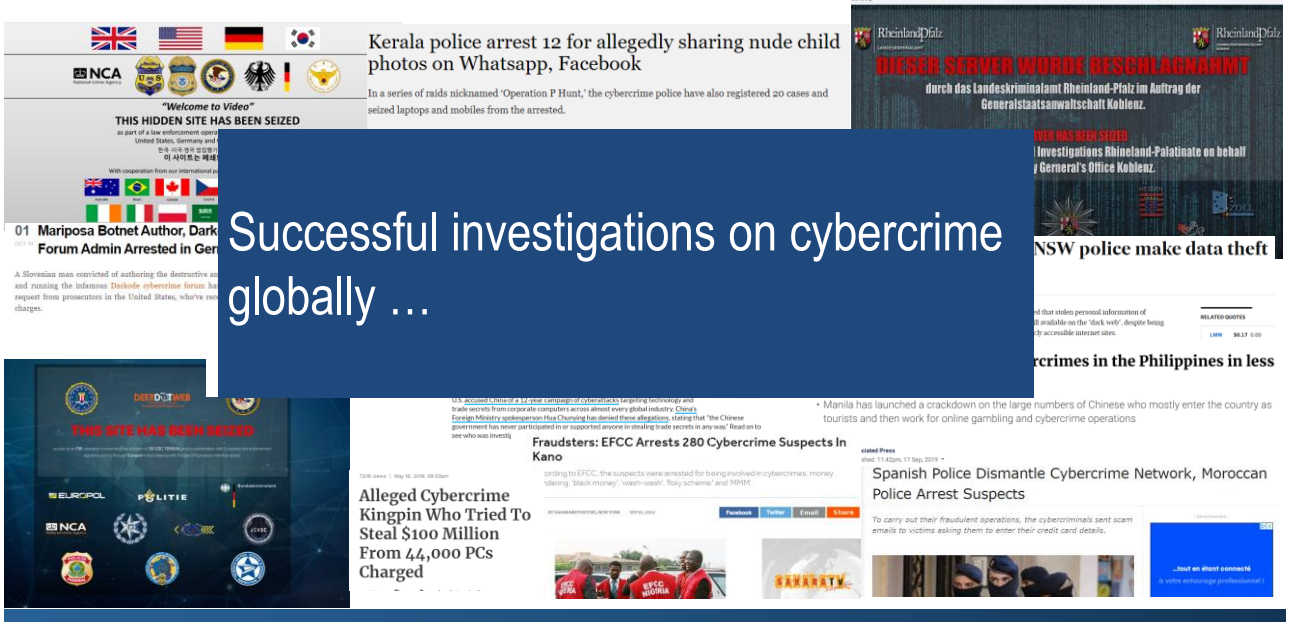
Cybercrime and e-evidence as matters of criminal justice

- Governments have an obligation to protect, including through criminal law (ECtHR 2008: K.U. v Finland)
- Cybercrime and e-evidence require an effective criminal justice response
- Budapest Convention is a criminal justice treaty (specified data in specific investigations)
- Criminal justice response is protective:
  - ▶ powers to investigate and prosecute
  - ▶ but limited by rule of law conditions and safeguards to protect rights of individuals, including suspects, and prevent abuse

Question: How relevant, how effective is the criminal justice response?

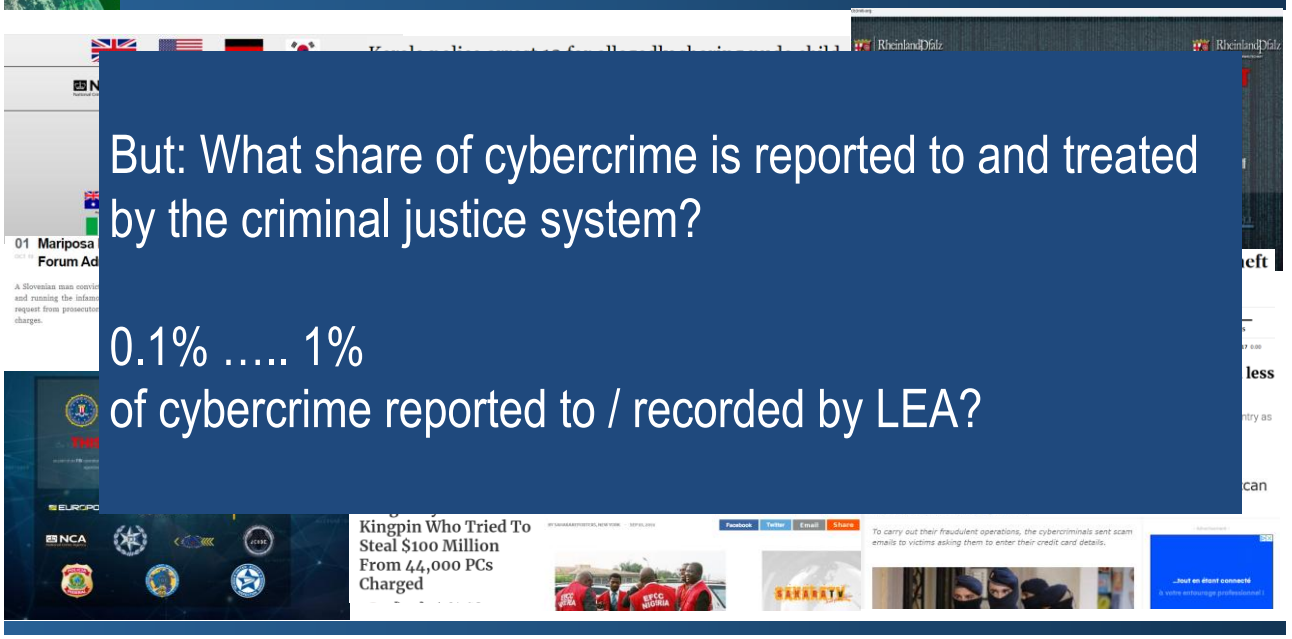
5

Cybercrime and e-evidence as matters of criminal justice



6

Cybercrime and e-evidence as matters of criminal justice



But: What share of cybercrime is reported to and treated by the criminal justice system?

0.1% ….. 1%
of cybercrime reported to / recorded by LEA?

7

Cybercrime and e-evidence as matters of criminal justice

0.1% ….. 1% of cybercrime reported to / recorded by LEA?

WHY?

- Criminal justice too complicated, not efficient, “useless”?
- Attacks against industry and institutions considered matter of national security?
- Self-defence?
- Reputation?
- Insurance pays?
- Unclear legislation and responsilities of LEA (cyberviolence)?
- …..

8

Cybercrime and e-evidence as matters of criminal justice

From the 0.1 – 1% of cybercrime that is reported to LEA….

How much is
⇩
Investigated: %?
⇩
Prosecuted: %?
⇩
Adjudicated: 1%?

⇒ **WHY?**

= 0.001 – 0.01 % of all cybercrime with a conclusive criminal justice response?

= From 100,000 crimes ► 100 – 1,000 reported to / recorded by LEA ► 1 – 10 convictions?

Note: this does not yet include other offences involving electronic evidence.

9

Why 1% adjudicated?

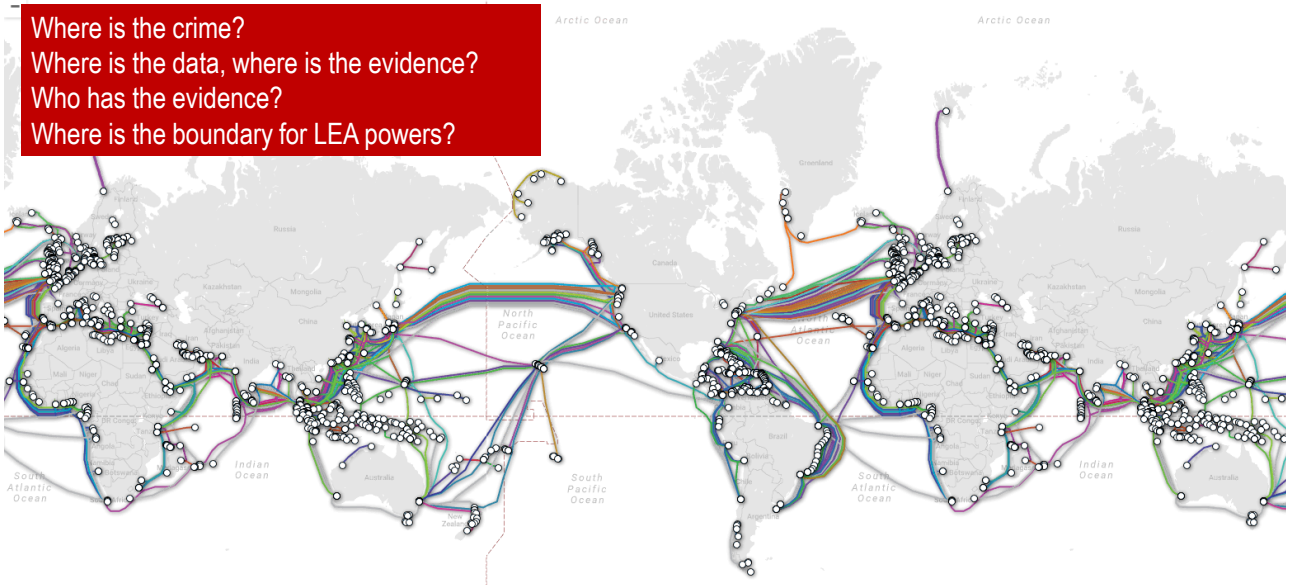
Cybercrime and electronic evidence: challenges for criminal justice:

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
  - Cloud computing: distributed systems ▶ distributed data ▶ distributed evidence
  - Unclear where data is stored and/or which legal regime applies
  - Service provider under different layers of jurisdiction
  - Unclear which provider for which services controls which data
  - Is data stored or in transit ▶ production orders, search/seizure or interception?
- The challenge of mutual legal assistance
- No data ▶ no evidence ▶ no justice

10

Why 1% adjudicated?

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



11

0.01 – 0.001%: What consequences?

- Do we have a rule of law problem in cyberspace?
- Do governments meet their obligation to protect (K.U. v. Finland)?
- Primary government response through cybersecurity, national defence and national security institutions?
- Residual response through criminal justice?
- Strict rule of law and data protection safeguards for criminal justice v. “margin of appreciation” for national security response (bulk interception, “mass surveillance”?

12

0.01 – 0.001%: What consequences?

- Further shift of competencies from the ”cumbersome“ criminal justice (with strict safeguards) to the “more efficient” national security arena (with limited safeguards)?
- Limited reliance on criminal justice?
- Limited focus on victims?
- Shift from protecting individuals to protecting critical infrastructure?
- Erosion of trust in public institutions, democracy, and state governed by rule of law and protecting human rights?

13

0.01 – 0.001%: What consequences?

- Risk to free and open internet:
  - Credible solutions to security needed for the multi-stakeholder model of a free, open and lobal internet
  - (as opposed to a model of sovereign internets controlled by States)
  - (see also forthcoming UN AHC to negotiate a new treaty on criminal misuse of ICT)

14

Solutions?

Innovative solutions needed for more effective/efficient criminal justice response to crime online WITH human rights, rule of law and data protection safeguards

One such solution:

- Budapest Convention on Cybercrime with new Second Additional Protocol

15

The mechanism of the Budapest Convention

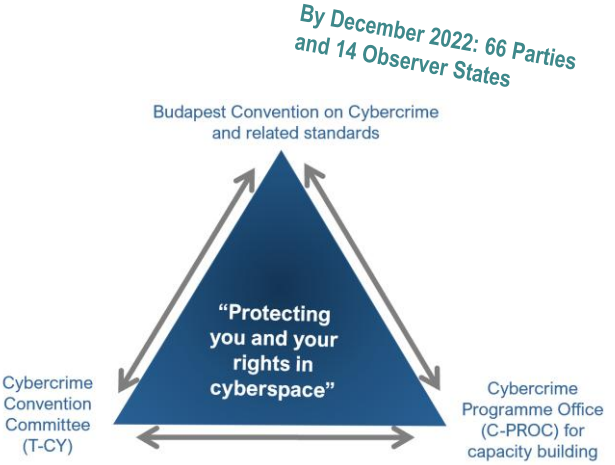
Budapest Convention on Cybercrime (2001):

1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence (adopted 17 November 2021)



16

Reach of the Budapest Convention

- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 14 signatories and States invited to accede
- ✓ 120+ States with substantive laws aligned with BC
- ✓ 150+ States have been participating in COE activities on cybercrime
- ✓ Promoting rule of law and human rights in cyberspace

► **Multilateral instrument – the same expected from 2nd Protocol**

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

Cybercrime: Threat to

- ► Human rights
- ► Democracy
- ► Rule of law

Positive obligations:

- ► Provide the means to protect the rights of individuals, also against crime

Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- 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?

Specific issues:

- 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:

- ► [May 2022 – Opening for signature]

21

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

22

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

Example: Direct cooperation with service providers in other Parties

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

Article 7 on

► "Direct disclosure of subscriber information"

23

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.

24

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

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

25

2nd Additional Protocol to the Convention on Cybercrime: safeguards

Issue: Efficiency with 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

26

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)