KYOTO CONGRESS 2020

Fourteenth United Nations Congress on Crime Prevention and Criminal Justice
Kyoto, Japan
7-12 March 2021

Session #262 – Cooperation on cybercrime: Risks and safeguards

Organised by the Council of Europe in cooperation with the Government of Romania

Tuesday, 9 March 2021 (14h00-15h30 Kyoto / 6h00-7h30 Strasbourg)

Speakers:

- Cristina Schulman, Romania
- Camila Bosch Cartagena, Chile
- Jayantha Fernando, Sri Lanka
- Patricia Adusei-Poku, Ghana
- Alexander Seger, Council of Europe

Aim of the meeting:

Promote an effective criminal justice response to cybercrime and challenges of electronic evidence with human rights and rule of law safeguards

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

The challenge

Alexander Seger
Head of Cybercrime Division
Council of Europe

Cybercrime and e-evidence: Failure to protect?

- 1% of cybercrime reported to criminal justice?
- 1% of cases reported resulting in convictions?
- What % of all other crime where evidence is on a computer system?

- Problem of rule of law in cyberspace?
- Do governments meet their obligation to protect individuals against crime?
- Can victims expect justice?
- Primary response by national security bodies; residual response by criminal justice system?

The challenge

Less than 1% of cybercrime reported to / recorded by LEA?

WHY?

- Criminal justice too complicated, too many safeguards, 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)?
- .....

From 1% of cybercrime reported to LEA, only 1% adjudicated?

WHY?

- The scale and quantity of cybercrime, devices, users and victims
- Technical challenges (VPN, anonymisers, encryption, VOIP, NATs etc.)
- Cloud computing, territoriality and jurisdiction
- The challenge of mutual legal assistance
- Strict rule of law and data protection safeguards for criminal justice v. "margin of appreciation" for national security response?

- **Primary government response through cybersecurity, national defence and national security institutions?**
- **Residual response through criminal justice?**

The challenge

Rule of law requirements for investigative measures interfering with rights of individuals:

- must be prescribed by law and the law must meet the requirements of precision, clarity, accessibility and foreseeability;
- must pursue a legitimate aim;
- must be necessary, that is, it must respond to a pressing social need in a democratic society and thus be proportionate;
- must allow for effective remedies;
- must be subject to guarantees against abuse.

The key challenge:

How can we provide for an effective criminal justice response to cybercrime and electronic evidence and for cooperation at all levels with human rights and rule of law safeguards?

Ingredients of a response

Cristina Schulman
Chair of the
Cybercrime Convention Committee
Ministry of Justice of Romania

A criminal justice framework based on the Budapest Convention on Cybercrime:

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

Harmonisation

Currently

- **77 Parties, Signatories and States invited to accede**
- **140+ countries have used it as a guideline for domestic legislation**

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

Ingredients of a response

In preparation:

2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence

- Legal basis for disclosure of WHOIS information
- Basis for direct cooperation with service providers in other Parties 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.

- A more effective criminal justice response to cybercrime and challenges of e-evidence with rule of law safeguards
- Respect for free Internet with limited restrictions in case of criminal misuse ≠ State control of information in cyberspace

Ingredients of a response

Risk: Overbroad criminalisation

- restricting freedom of expression
- facilitating State control of information in cyberspace

Risk: Procedural powers without appropriate safeguards

Safeguards in Budapest Convention + 2nd Additional Protocol

- Criminalisation: specific offences
- Embedded within criminal law framework
- Legal basis for specific criminal investigations where specified data is needed (≠ mass surveillance or bulk collection of data)
- Judicial or other independent supervision
- Grounds for refusal, use limitation, reservations
- Etc.

+ data protection safeguards

Experiences: Chile

Camila Bosch Cartagena
Chile

- What is needed in terms of public/private and international cooperation – experience of Chile/Latin America

E-evidence is no longer stored in devices – a lot of the information is stored in THE CLOUD

Apps, social networks, email accounts… means by which crimes are commited or good sources for evidence

Service Providers have stored in there servers electronic data that can be valuable evidence

For countries in Latin America, the mayority of SP are located abroad

While we don't have a legal framework that helps…

Experiences: Chile

- What is needed in terms of public/private and international cooperation – experience of Chile/Latin America

Direct cooperation with service providers:

Law enforcement guides – Chile, Argentina, Peru …

Each SP cooperates on there own terms … important to check their online guides

Preservation + suscriber information (art. 18 p 3 of the Budapest Convention)

If the SP doesn't cooperate: 24/7 Network of the Budapest Convention for preservation of electronic evidence

Experiences: Chile

- What is needed in terms of public/private and international cooperation – experience of Chile/Latin America

Thank you!

camilaboschcar@gmail.com

Experiences: Sri Lanka

Jayantha Fernando
Director/ Legal Advisor at the ICT Agency of Sri Lanka (ICTA) and Director, Sri Lanka CERT

Road to Budapest Convention

- Sri Lanka Invited to accede to Budapest Cybercrime Convention - 23rd February 2015 (process started in 2008)
- Acceded to the Cybercrime Convention (29th May 2015)
  - Applicable on Sri Lanka – w.e.f - 1st September 2015
- **1st Country in South Asia** & 2nd in Asia after Japan
  - Fastest accession in Council of Europe
- Journey towards accession was a strategy under "***e-Sri Lanka Development Program***" – The 1st Digital Strategy :-
  - Regulatory and Law reform based on "International Standards"
  - Capacity building measures – Law Enforcement & Judicial Training

Experiences: Sri Lanka

Sri Lankan Legal Framework & How it helped address challenges

- Primary Legislation – Computer Crimes Act No. 24 of 2007
  - Substantive Cybercrime offences
  - Procedural measures to obtain BSI and Traffic Data with Safeguards
  - Mutual Legal Assistance Act – incorporated by Reference
- **Other Legislative and Inter-connected measures**
  - PAYMENT DEVICES FRAUDS ACT, No. 30 OF 2006
  - Intellectual Property Act, No. 36 Of 2003
  - Recommendations of Financial Action Task Force (FATF)
  - Penal Code Amendments (1995) and (2006) –Online Child Pornography
  - **ICCPR Act (2007) – Offences against Hate Speech etc**
  - Mutual Legal Assistance in Criminal Matters Act No. 25 /2002 (Amended Act 24 of 2018)
- **Addressing Challenges through Budapest Convention**
  - Enforcement capacity? International cooperation - Delays?
  - Gathering and presenting Electronic evidence
  - Challenges addressed through Capacity Building programs and Institutional Reform
  - Easter Sunday Incident and aftermath

Experiences: Sri Lanka

Developing Capacity and Institutional frameworks

- **Effective Capacity Building Measures**
  - Judicial, Prosecution, & Police Capacity buildng through GLACY + Program
  - ToT for Judicial authorities & adoption of e-Evidence Guide (321 Judges trained) – ***International Coop, e-Evidence & Data Privacy***
  - Over 650 Police officer trained through CID Cybercrime Unit (GLACY +)
  - Digital Forensic Labs & Adoption of SOPs for e-evidence
  - Judicial Delegation led by Chief Justice– Training for Nepal Judges (2017)
  - South-South Cooperation - support for Cybercrime Legislation in Fiji

- Sri Lanka CERT – www.cert.gov.lk
  - National CERT established (full member of FIRST and APCERT)
  - Sector specific CSIRTS (eg:- **FinCERT)**
  - Facilitates effective Public private cooperation & Expert assistance for digital forensics
  - Effectiveness enhanced by GLACY+ & Cyber4Dev projects

Experiences: Sri Lanka

2021: Benefits of Cybercrime Convention Committee (T-CY)

Guidance Notes - Common understanding of the Parties on how to apply the Convention and address new phenomena

Guidance Notes on :

- **"botnets", distributed denial of service attacks"**
- **"identity theft and phishing in relation to fraud"**
- **"new forms of malware"**
- **"transborder access to data (Article 32)" / "spam"**
- **Article 18 "Production Order" etc & Cloud Evidence Group - Report**

Additional Protocol to the Convention

- **Bigger Role for Parties in PDG / PDP**
- **Benefits of Participation**
- **Sri Lanka's fast track Drafting of Data Protection Legislation**

The Budapest Convention remains relevant as crimes evolve and benefits Parties from participating in T-CY

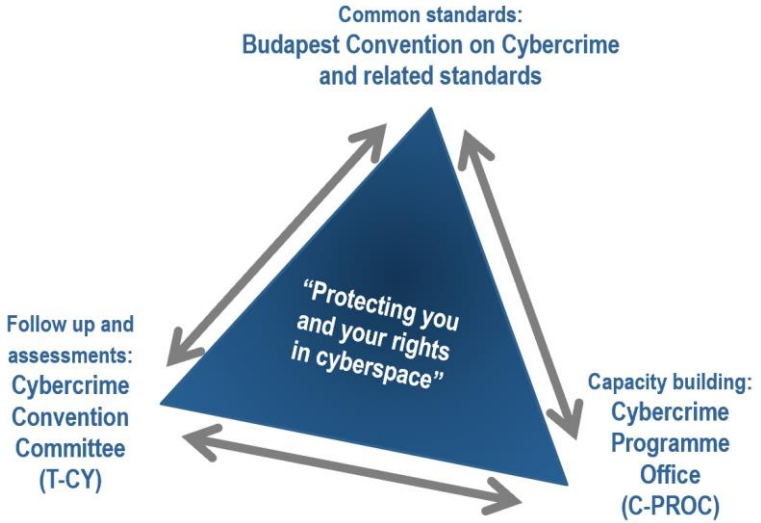
Experiences: Data protection in Africa

Patricia Adusei-Poku
Executive Director of the
Ghana Data Protection Commission

- Need for data protection safeguards also within criminal justice context
- Experience of Ghana
- Developments in Africa

Take-aways

- Continue reforms of domestic legislation in terms of specific criminalisation and procedural powers subject to conditions and safeguards ► Budapest Convention on Cybercrime as a model/guideline
- Enhanced cooperation and disclosure of electronic evidence to ensure a more effective criminal justice response to cybercrime to ensure the rule of law in cyberspace ► Budapest Convention + future 2nd Protocol Budapest Convention as a framework
- Access to evidence in a cross-border/cloud context raises complex questions related to territoriality, jurisdiction and the protection of fundamental rights ► Specific safeguards of Budapest Convention + 2nd Protocol (also Council of Europe data protection Convention 108+)
- Capacity building remains a most effective means to enable a more effective criminal justice response to the challenges of cybercrime and e-evidence ► Experience of C-PROC



Additional international treaties on cybercrime need to:

- Be based on broad consensus to avoid further polarization/divisions
- Meet the needs of criminal justice practitioners
- Meet human rights and rule of law requirements
- Be compatible with existing instruments