Informal TC-INF on Cybercrime

23 November 2018, 15h30-17h00, Council of Europe (AGORA G3)

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cybercrime and e-evidence: Update on current challenges and the COE response

Alexander Seger
Head of Cybercrime Division
Council of Europe
alexander.seger@coe.int

Cristina Schulman
Chair
Cybercrime Convention Committee (T-CY)
Romania

www.coe.int/cybercrime

Cybercrime and electronic evidence: CONTEXT

Cybercrime and e-evidence: increasing and transversal challenges that affect human rights, democracy and the rule of law:

- **Scale and complexity versus criminal justice capacities and resources**
- **How to reconcile security and fundamental rights**
- **Preference to criminal justice approach but ….**

Council of Europe response:

- **Budapest Convention and Protocol XR**
- **Capacity building (C-PROC)**
- **T-CY work on Protocol**

Considerations:

- **Political fragmentation and diverging interests in cyberspace**
- **EU e-evidence proposals**
- **Developments at UN**

Cybercrime and electronic evidence: challenges

Cybercrime and e-evidence are transversal challenges that affect human rights, democracy and the rule of law

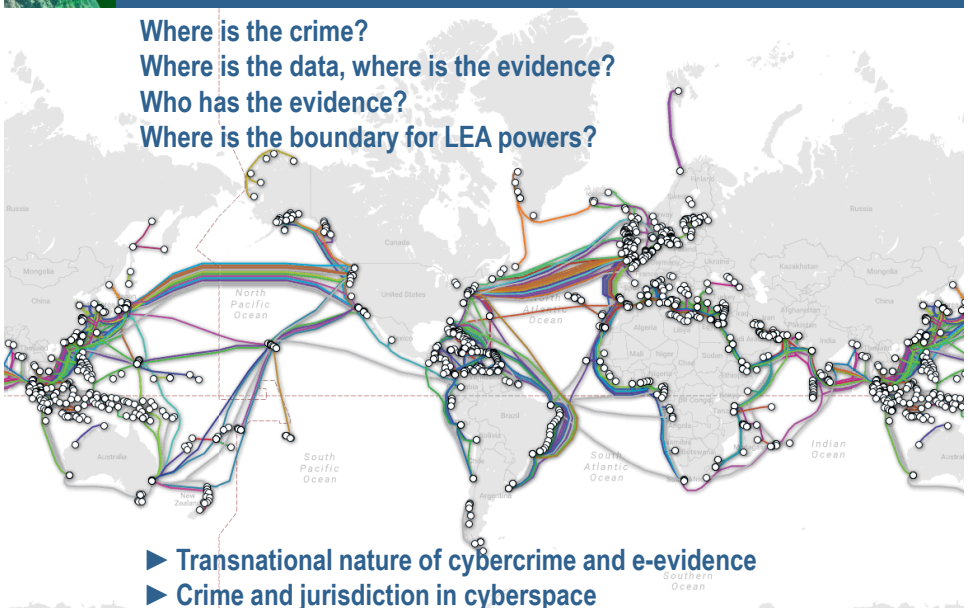
- Ransomware (WannaCry, NotPetya)
- DDOS
- Critical information infrastructure attacks
- Election interference
- Data breaches
- Cyberviolence
- Child sexual abuse materials
- Fraud
- Cryptocurrencies (means and targets of crime)
- Darkmarkets
- Social engineering
- Etc.

Issues:

- Technology (Static vs dynamic IP addresses, encryption, VPN, NATs, IoT etc.)
- Criminals or Governments?
- Cybercrime or cyberwarfare?
- Criminal justice or national security / defence?
- Security or fundamental rights?
- Data protection or crime prevention and criminal justice?
- Territoriality of criminal justice versus crime and evidence in the cloud?

Example: Crime and evidence in the cloud

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

Challenge: Are governments able to protect?

Cybercrime = ?

↓

Reported to/recorded by police = 100

↓

Investigated

↓

Prosecuted

↓

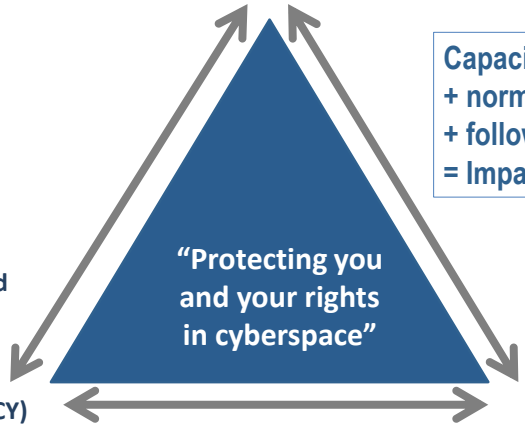
Adjudicated = 10 or 1 or 0.1 or 0.01?

↓

= Cyberspace basically safe, crime the exception, offenders brought to justice, individuals and their rights protected?
= Rule of law in cyberspace?
= Do govs meet obligation to protect individuals against crime (ECtHR, K.U. v. Finland)?

The Council of Europe approach: Criminal justice response with safeguards

1 Common standards: Budapest Convention on Cybercrime, Protocol XR and relates standards



Capacity building
+ normative standards
+ follow up mechanism
= Impact + dynamics

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

3 Capacity building: C-PROC ▶ Technical cooperation programmes

Scope of 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
- Search and seizure
- Production orders
- 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

Scope of Budapest Convention

Cybercrime

- Offences against computer systems and data
- Offences by means of computer systems and data

Electronic evidence

- Any crime may involve evidence in electronic form on a computer system
- Needed in criminal proceedings
- No data, no evidence, no justice

www.coe.int/cybercrime

Convention complemented by …

- Protocol on Xenophobia and Racisms via Computer Systems
  (31 Parties + 13 Signatories)
- Guidance Notes on
  - Notion of computer systems
  - Botnets
  - Malware
  - Spam
  - Terrorism
  - Transborder access to data (Article 32)
  - Production Orders for Subscriber Information (Article 18)
  - Etc.
- [Protocol on enhanced international cooperation under negotiation]

= Budapest Convention remains up-to-date and relevant

Example: Cybercrime and other offences in the election process - the role of the Budapest Convention

Attacks against the confidentiality, integrity and availability of election computers and data

- Compromising voter databases or registration systems
- Tampering with voting machines to manipulate results
- Interference with the function of systems
- Illegal access to computers to steal, modify, disseminate sensitive data for information operations

Information operations with violations of rules to ensure free, fair and clean elections

- Data protection rules
- Rules on political finances
- Rules on media coverage of electoral campaigns
- Rules on broadcasting and political advertising

Budapest Convention

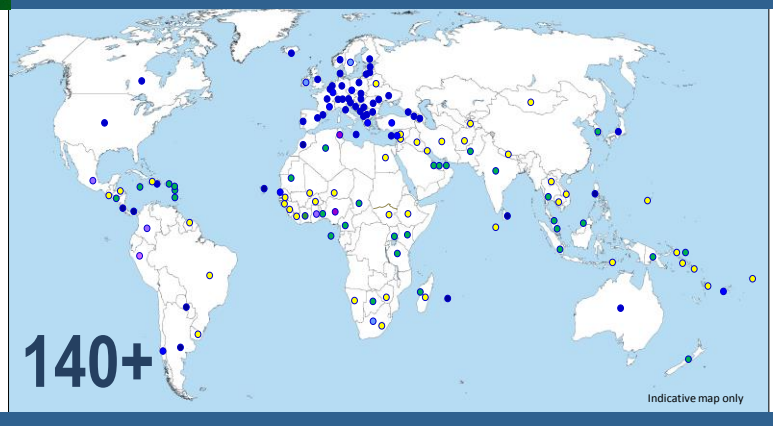
Substantive criminal law provisions

- Article 2 Illegal access
- Article 3 Illegal interception
- Article 4 Data interference
- Article 5 System interference
- Article 6 Misuse of devices
- Article 7 Forgery
- Article 8 Fraud
- Article 11 Attempt, aiding, abetting

Procedural powers and international cooperation to secure electronic evidence and prosecute offenders

- Articles 16, 17, 29 and 30 for data preservation
- Article 18 Production orders
- Article 19 Search and seizure
- Etc. (incl. cooperation with service providers

Reach of the 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 = 50+

Impact > Legislation on cybercrime AND electronic evidence: Progress 2013 – 2018 re substantive criminal law

By January 2013	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	6	11%	18	33%	30	56%
All Americas	35	10	29%	12	34%	13	37%
All Asia	42	13	31%	17	40%	12	29%
All Europe	48	38	79%	8	17%	2	4%
All Oceania	14	3	21%	6	43%	5	36%
All	**193**	**70**	**36%**	**61**	**32%**	**62**	**32%**

By January 2018	States	Largely in place		Partially in place		Not in place or no information	
All Africa	54	14	26%	21	39%	19	35%
All Americas	35	14	40%	15	43%	6	17%
All Asia	42	17	40%	18	43%	7	17%
All Europe	48	44	92%	4	8%	0	0%
All Oceania	14	5	36%	6	43%	3	21%
All	**193**	**94**	**49%**	**64**	**33%**	**35**	**18%**

Legislation on cybercrime AND electronic evidence: Progress 2013 – 2018 re procedural powers

Specific procedural powers		In January 2013		In January 2018	
	States	Largely in place		Largely in place	
All Africa	54	5	*9%*	10	*19%*
All Americas	35	5	*14%*	9	*26%*
All Asia	42	8	*19%*	13	*31%*
All Europe	48	31	*65%*	39	*81%*
All Oceania	14	1	*7%*	3	*21%*
All	**193**	**50**	***26%***	**74**	***38%***

Effectiveness/Impact of the Budapest Convention

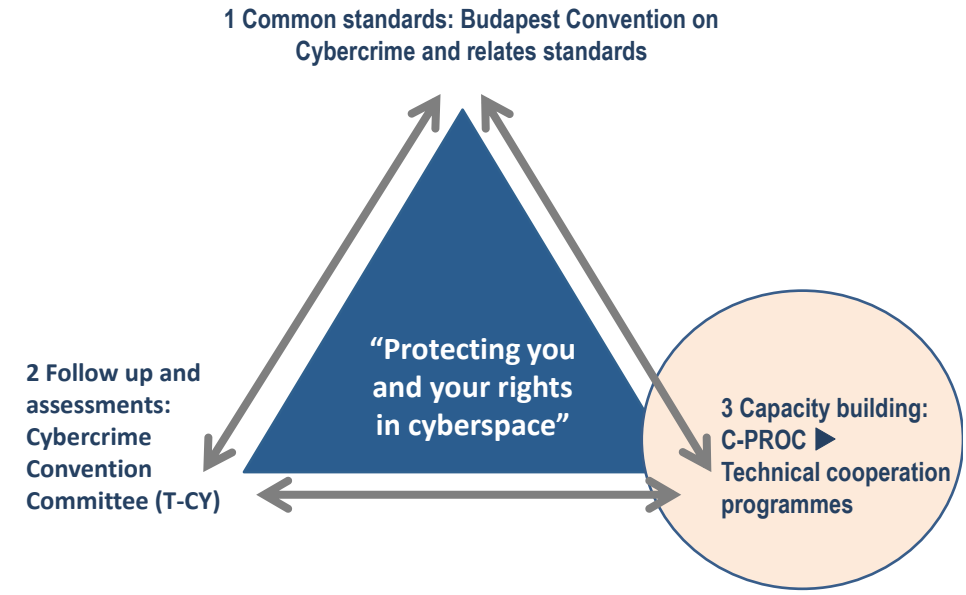
- Stronger and more harmonised legislation
- More efficient international cooperation between Parties
- Better cybersecurity performance
- More investigation, prosecution and adjudication of cybercrime and e-evidence cases
- Trusted partnerships and public/private cooperation
- Catalyst for capacity building
- Contribution to human rights/rule of law in cyberspace

= "Protecting you and your rights"

The Budapest Convention is in place and functioning.

15

The Council of Europe response: Capacity building by C-PROC



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

- February 2013: UN Expert Group on Cybercrime – "broad agreement on capacity building", "diverse views" on other solutions
- Committee of Ministers decision on C-PROC October 2013
- Operational as from April 2014
- Currently 29 staff + 5 programmes (ca. EUR 27 million, 200+ activities per year)

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

Current capacity building programmes

- **GLACY+** EU/COE Joint Project on Global Action on Cybercrime Extended
- **Cybercrime@EAP 2018** EU/COE Eastern Partnership on international cooperation
- **iPROCEEDS** EU/COE cooperation on Cybercrime: targeting proceeds from online crime in South-eastern Europe
- **Cybercrime@Octopus** (voluntary contribution funded)
- **CyberSouth** EU/COE project for the Southern Neighbourhood

C-PROC capacity building – examples of recent activities

- 1 – 2 November 2018, Kyiv, Ukraine – Advisory Mission on international cooperation through 24/7 points of contact and mutual legal assistance, Cybercrime@EAP2018
- 5 – 7 November 2018, Budapest, Hungary – Training on financial frauds and virtual currencies in cooperation with the, International College of Financial Investigations, iPROCEEDS
- 5 – 9 November 2018, Chile - Introductory Judicial ToT on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers and adaptation of materials, GLACY+
- 7 – 8 November 2018, Algiers, Algeria – Study visit for specialized units, CyberSouth
- 12 – 14 November 2018, Tunis, Tunisia – Basic judicial Training, CyberSouth
- 12 – 14 November 2018, Bucharest, Romania – Regional workshop on Business E-mail Compromise, credit card fraud and e-commerce fraud, CyberSouth
- 12 – 15 November 2018, Bucharest, Romania - Regional case simulation exercise on cybercrime and financial investigations, iPROCEEDS
- 12 – 15 November 2018, Morocco - ECTEG Course, Cybercrime and digital forensics specialized training for law enforcement officers, GLACY+
- 12 – 15 November 2018, Senegal - Advanced Judicial Training on cybercrime and electronic evidence for Judges, Prosecutors and Lawyers with participation of Francophone and Lusophone countries from the ECOWAS Region, GLACY+

20

C-PROC capacity building – examples of recent activities

- 13 November 2018, the Netherlands – Presentation on the Budapest Convention at the ENISA-EC3 Workshop on CSIRT and international law enforcement cooperation, GLACY+
- 13 – 14 November 2018 , Bucharest, Romania – Seminar "Investigating Web 2.0 - The Collection of Evidence Located Abroad and the Challenges of Transborder Access to Data", organized by ERA and NIM (National Institute for Magistracy), GLACY+
- 14 – 16 November 2018, Sri Lanka – In-country workshops on data protection and INTERPOL Tools and Services combined with support on how to set-up and how to strength the 24/7 points of contact for cybercrime and electronic evidence, GLACY+
- 15 November 2018, Beirut, Lebanon – Round table on cybersecurity strategy, CyberSouth
- 16 November 2018, Beirut, Lebanon – Awareness meeting on Budapest Convention, CyberSouth
- 15 – 16 November 2018, Bucharest, Romania - Human Rights Workshop with the Fundamental Rights Agency, GLACY+

C-PROC capacity building – conclusions and way ahead

- COE a global leader for capacity building
- Unique approach of dynamic triangle (including support to T-CY)
- Enhances application of Budapest Convention in practice
- Resource mobilisation
- Support by EU and multiple partners

Way ahead:

- Emphasis on rule of law and human rights, incl data protection, safeguards
- Further enhancing application of Budapest Convention and its Protocols in practice
- Protecting children
- Follow up to study on cyberviolence
- Resource mobilisation + new projects for EaP and South-eastern Europe
- C-PROC as centre of expertise

Towards a new Protocol to the Budapest Convention

Context:

Budapest Convention on Cybercrime ► Cybercrime Convention Committee (T-CY) ► Cloud Evidence Group ► Recommendations September 2016 ► now under consideration by T-CY

Rationale:

- Cybercrime AND electronic evidence in relation to any crime
- E-evidence on servers in foreign, unknown, multiple or shifting jurisdictions, in the cloud
- No data, no evidence, no prosecution, no justice, no rule of law (in cyberspace)

Issues:

- Differentiating subscriber versus traffic versus content data
- Limited effectiveness of MLA
- Loss of location and transborder access jungle
- Provider present or offering a service in the territory of a Party
- Voluntary disclosure by US-providers
- Emergency procedures
- Data protection

Solutions:

1. More efficient MLA
2. Guidance Note on Article 18
3. Domestic rules on production orders (Article 18)
4. Cooperation with providers: practical measures
5. Protocol to Budapest Convention

Example: Direct cooperation with providers across jurisdictions

	Requests for data directly sent to Apple, Facebook, Google, Microsoft, Twitter and Oath in 2017		
Parties and Observers (70 States)	Received	Disclosure	%
Albania	27	14	53%
Argentina	4 979	3 636	73%
Australia	6 555	4 543	69%
Belgium	2 521	2 301	91%
Canada	1 928	1 567	81%
Chile	1 488	1 094	74%
France	29 400	18 466	63%
Germany	35 596	20 172	57%
Italy	9 736	5 521	57%
Japan	3 822	2 598	68%
Netherlands	3 338	2 773	83%
Portugal	3 569	2 394	67%
Spain	6 353	3 418	54%
United Kingdom	31 954	23 073	72%
Total (excluding USA)	170 680	109 093	64%

Protocol to the Budapest Convention on Cybercrime

A. Provisions for more efficient MLA
- Emergency MLA
- Joint investigations
- Video conferencing
- Language of requests
- Etc.

B. Provisions for direct cooperation with providers in other jurisdictions

C. Framework and safeguards for existing practices of extending searches transborder

D. Safeguards/data protection

Terms of reference approved in June 2017.

Negotiations: Sep 2017 – Dec 2019.

Outlook 2019

- Cybercrime and e-evidence are transversal matters
- Relevance of Budapest Convention will continue to increase
- Preparation of Protocol to the Budapest Convention
- EU E-Evidence Regulation and Directive
- Criminal justice in cyberspace – Conference organised by the Romanian Presidency of the EU Council and the Council of Europe (combined with 5th anniversary of C-PROC) – February 2019
- Octopus Conference November 2019
- UN: UNIEG, Crime Commission (CCPCJ) and UNGA?


Questions?
www.coe.int/cybercrime