OCTOPUS CONFERENCE
Strasbourg, 20-22 November 2019

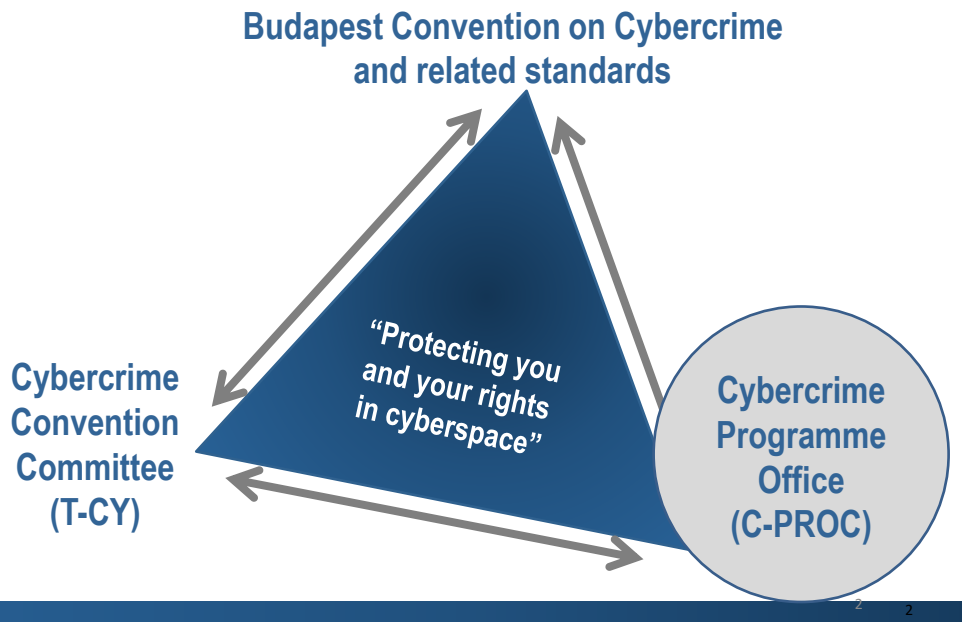
Results of capacity building and impact on legislation

Alexander Seger
Head of Cybercrime Division
Council of Europe

www.coe.int/cybercrime

1

Capacity building in cybercrime and e-evidence: Council of Europe approach



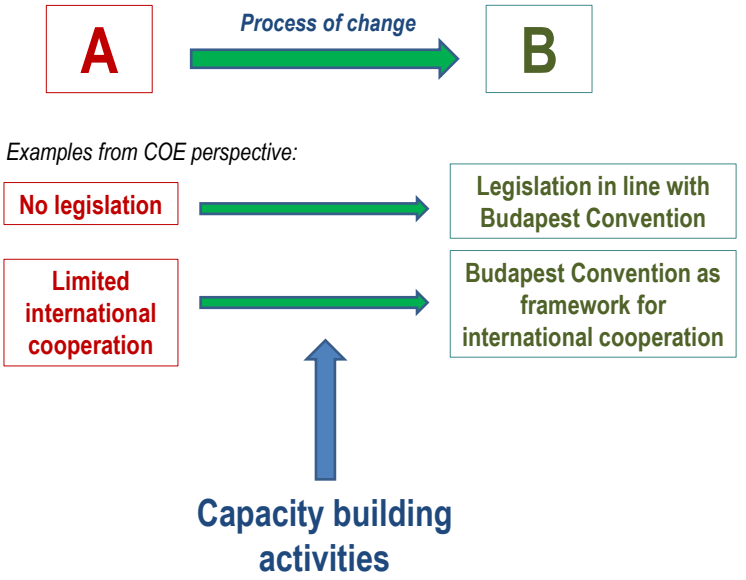
2

About capacity building

"Capacity building" = enabling criminal justice authorities to meet the challenge of cybercrime and electronic evidence.

This entails strengthening the knowledge and skills and enhancing the performance of criminal justice organisations including their cooperation with other stakeholders.

It should be aimed at protecting individuals and society against crime and at protecting the rights of individuals, at promoting security, confidence and trust in ICT, at strengthening human rights, democracy and the rule of law in cyberspace and at contributing to human development.



3

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
  - ► Decision to establish C-PROC
- Task: Support to countries worldwide to strengthen criminal justice capacities on cybercrime and electronic evidence
- Operational as from April 2014
- Currently 30 staff + 6 programmes (ca. EUR 32 million)
- 240 activities during past 12 months, 850+ activities since 2014

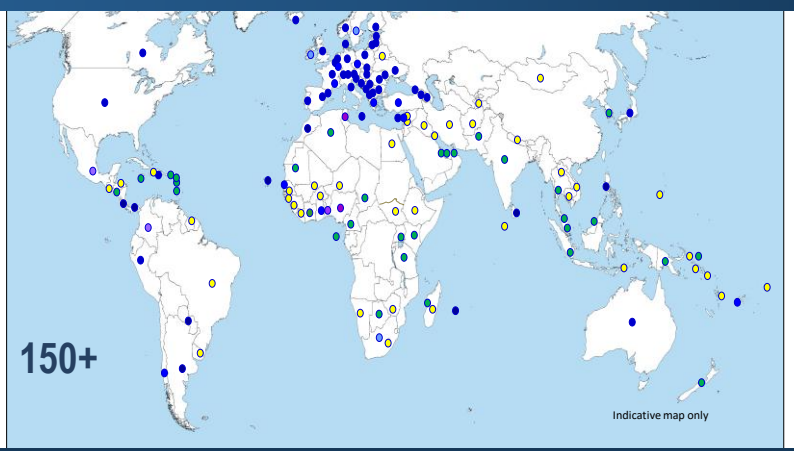
4

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

Cybercrime@Octopus	Jan 2014 – Dec 2020	EUR 4 million	Voluntary contributions
GLACY+ project on Global Action on Cybercrime Extended	Mar 2016 – Feb 2021	EUR 13.35 million	EU/CoE JP
iPROCEEDS project targeting proceeds from crime on the Internet in South-eastern Europe and Turkey	Jan 2016 – Dec 2019	EUR 5.56 million	EU/CoE JP
EndOCSEA@EUROPE project against Online Child Sexual Exploitation and Abuse	July 2018 – Dec 2020	EUR 0.85 million	End Violence against Children Fund
CyberSouth on capacity-building in the Southern Neighbourhood	July 2017 – June 2020	EUR 3.33 million	EU/CoE JP
CyberEast Project on Action on Cybercrime for Cyber Resilience in the Eastern Partnership region	June 2019 – June 2022	EUR 4.22 million	EU/CoE JP

5

Reach of the Budapest Convention / reach of C-PROC capacity building



Parties: 64
Signed: 3
Invited to accede: 5
= 72

Other States with laws largely in line with Budapest Convention = 20+
Further States drawing on Budapest Convention for legislation = 50+

6

Impact of capacity building

- Works, responds to needs and makes an impact
  - Legislation with safeguards
  - Investigations and criminal proceedings
  - Public/private, interagency and international cooperation
  - Sustainable training
- Facilitates multi-stakeholder cooperation and synergies
- Has human development benefits and feeds into Sustainable Development Goals
- Helps reduce the digital divide
- Is based on broad international support and may help overcome political divisions

7

The global state of cybercrime legislation

The global state of

cybercrime legislation 2013 – 2019:

A cursory overview

Update as at 30 June 2019
prepared by the
Cybercrime Programme Office
of the Council of Europe (C-PROC)

8

The global state of cybercrime legislation

Reforms of legislation on cybercrime and electronic evidence in most UN m/s in recent years

		Reforms underway or undertaken in recent years					
	States	By January 2013		By January 2018		By June 2019	
All Africa	54	25	46%	45	83%	46	85%
All Americas	35	25	71%	31	89%	32	91%
All Asia	42	34	81%	37	88%	38	90%
All Europe	48	47	98%	48	100%	48	100%
All Oceania	14	12	86%	12	86%	13	93%
All	**193**	**143**	**74%**	**173**	**90%**	**177**	**92%**

9

The global state of cybercrime legislation

Substantive criminal law in line with Budapest Convention

	States	Largely in place by January 2013		Largely in place by June 2019	
All Africa	54	6	11%	18	33%
All Americas	35	10	29%	15	43%
All Asia	42	13	31%	18	43%
All Europe	48	38	79%	45	94%
All Oceania	14	3	21%	4	29%
All	193	70	36%	100	52%

10

Comment on substantive criminal law:

- ► Good practices available
- ► Concern: Laws on cybercrime used to prosecute speech

- The protection of national security and public order is a legitimate ground for restricting freedom of expression where that restriction is
  - prescribed by law
  - necessary in a democratic society
  - proportionate
- Broad, vaguely defined provisions do not meet these requirements
  - "use of computers with intent to compromise the independence of the state or its unity, integrity, safety or any of its high economic, political, social, military or security interests or subscribe, participate, negotiate, promote, contract or deal with an enemy in any way in order to destabilise security and public order or expose the country to danger …"
  - "use of computers to create chaos in order to weaken the trust of the electronic system of the state or provoke or promote armed disobedience, provoke religious or sectarian strife, disturb public order, or harm the reputation of the country … "
  - "creation of sites with a view to disseminating ideas contrary to public order or morality"
- Problematic trend ► Discredits legitimate action on cybercrime ► violates fundamental rights

11

The global state of cybercrime legislation

Specific procedural powers to secure electronic evidence

	States	By January 2013		By January 2018		By June 2019	
		Largely in place		Largely in place		Largely in place	
All Africa	54	5	9%	10	19%	15	28%
All Americas	35	5	14%	9	26%	12	34%
All Asia	42	8	19%	13	31%	13	31%
All Europe	48	31	65%	39	81%	40	83%
All Oceania	14	1	7%	3	21%	3	21%
All	**193**	**50**	**26%**	**74**	**38%**	**82**	**43%**

12

The global state of cybercrime legislation

Comment on procedural powers to secure electronic evidence

- Good practices available
- Increasing data protection regulations (Data Protection Convention 108 ► Cabo Verde, Mauritius, Morocco, Senegal + reforms in others)
- Often reliance on general powers
- Problem of safeguards

13

The global state of cybercrime legislation

		Use of Budapest Convention as guideline or source					
	States	By January 2013		By January 2018		By June 2019	
All Africa	54	21	39%	33	61%	38	70%
All Americas	35	22	63%	24	69%	25	71%
All Asia	42	25	60%	27	64%	28	67%
All Europe	48	46	96%	47	98%	47	98%
All Oceania	14	10	71%	11	79%	14	100%
All	**193**	**124**	**64%**	**142**	**74%**	**152**	**79%**

14

The global state of cybercrime legislation: Conclusions

- Criminalising attacks against and by means of computers:
  - Good progress
  - Some concerns over vague, broadly defined provisions
- Procedural powers to secure electronic evidence:
  - Progress in many countries
  - Progress in terms of data protection regulations
  - Specific, well-defined powers with conditions and safeguards still needed in a number of countries
- Budapest Convention on Cybercrime is relevant worldwide:
  - Used as guideline in an increasing number of countries
  - Some countries have joined or are joining to benefit from membership
- Legislation must be backed up by capacity building!