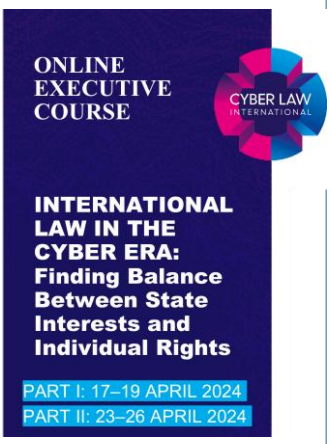
Human rights considerations in international cybercrime treaties



Human rights and rule of law considerations in:

- Budapest Convention on Cybercrime
- Draft UN treaty on cybercrime/ use of ICT for criminal purposes

Alexander Seger
Head of Cybercrime Division
Council of Europe
23 April 2024

COUNCIL OF EUROPE 75 1949 - 2024 CONSEIL DE L'EUROPE

Plan:

0. Cybercrime & e-evidence
1. About cybercrime treaties
2. Human rights considerations
3. Budapest Convention: conditions and safeguards
4. UN draft treaty: human rights and rule of law risks and solutions
5. Conclusions

Q & A after each section

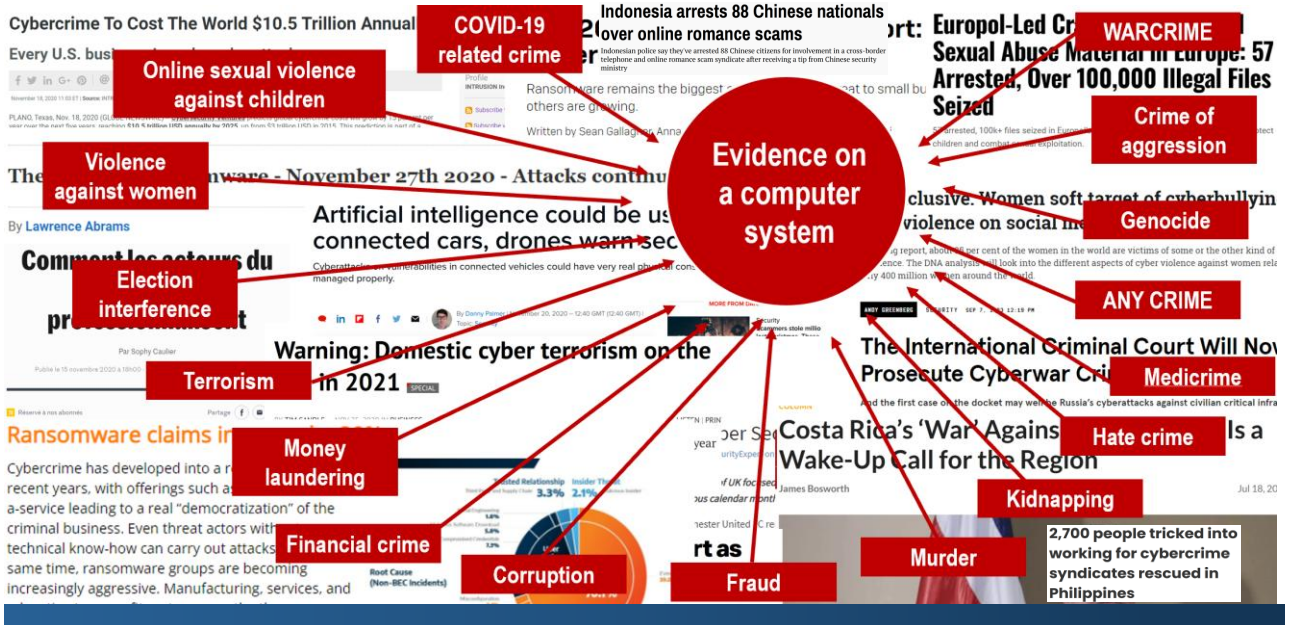
www.coe.int/cybercrime

1

Cybercrime …

2

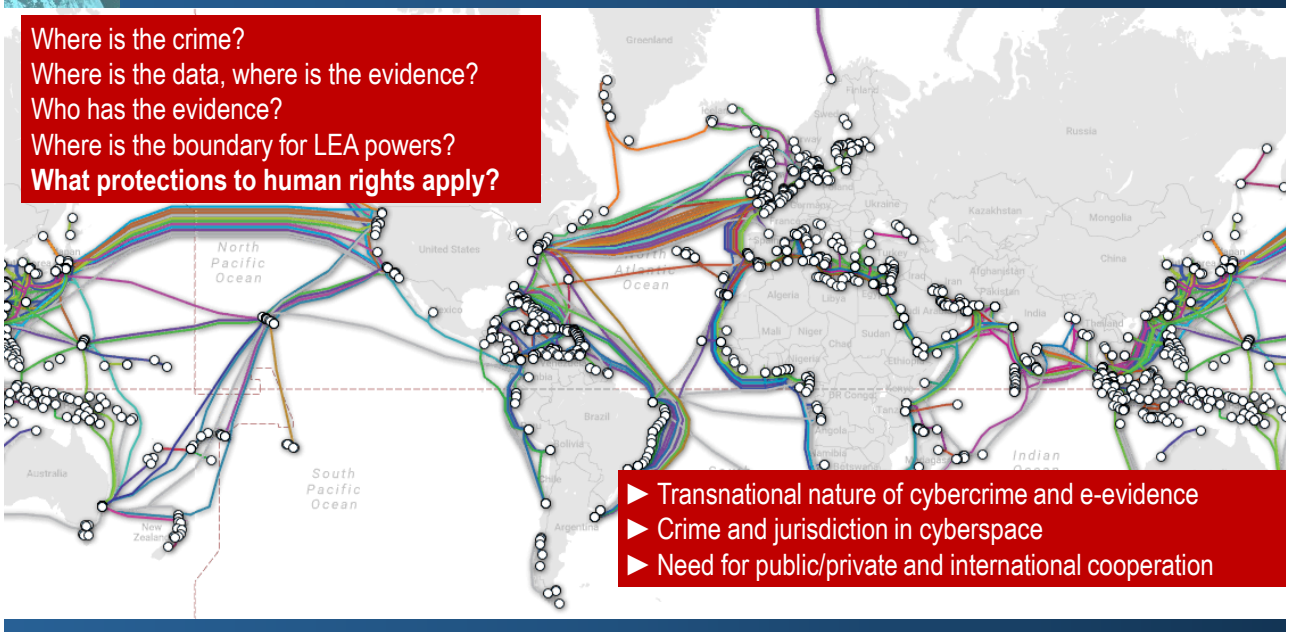
… and e-evidence re all types of crime



3

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?
What protections to human rights apply?



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

4

1. About cybercrime treaties

Human rights and rule of law conditions and safeguards in:

- Convention on Cybercrime (Budapest Convention 2001)
  - + First Protocol on xenophobia and racism (2003)
  - + Second Protocol on electronic evidence (2022)

- Proposal for a United Nations Convention on [Cybercrime / Use of information and communication technologies for criminal purposes]

[In preparation. UN AHC "**concluding concluding2** session [29 July – 9 August 2024 TBC]]

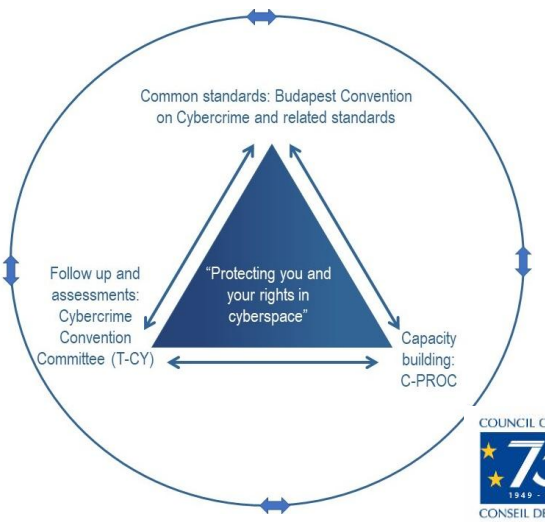
5

1. About cybercrime treaties: The framework of the Convention on Cybercrime

- Budapest Convention on Cybercrime (2001)
- 1st Protocol on Xenophobia and Racism via Computer Systems (2003)
- 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (2022)
- Guidance Notes

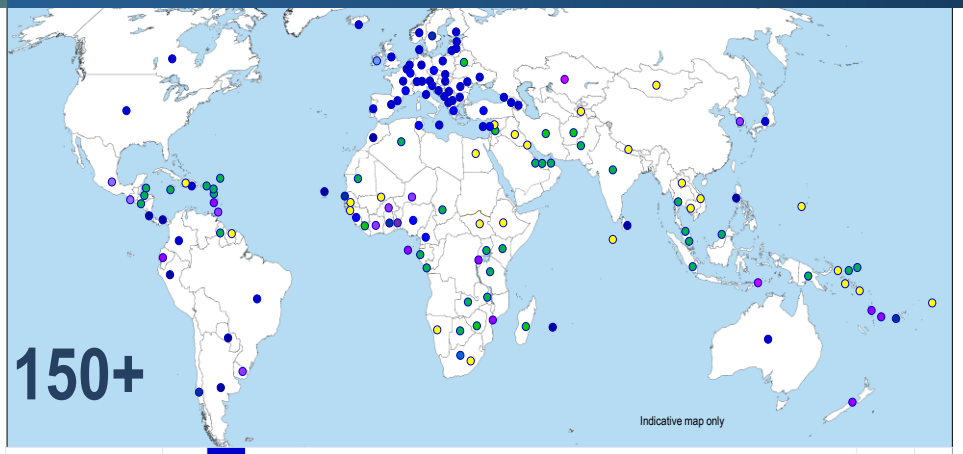
Cybercrime + electronic evidence !

By April 2024: **71 Parties and 22 Observer States**



6

Reach of the Convention on Cybercrime



Parties:	71			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	40+	
Invited to accede:	20	Further States drawing on Budapest Convention for legislation:	20+	
=	**93**	=	**60+**	

Parties include:

- Australia
- Japan
- Philippines
- Sri Lanka
- Tonga

7

1. About cybercrime treaties: Scope of the Convention on Cybercrime

Budapest Convention (2001):

1. Offences against and by means of computer systems (articles 2-12)
   - CIA offences (illegal access, data/system interference etc.), forgery and fraud, "child pornography", IPR
   - [Additional XR offences in First Protocol]
2. Procedural powers to investigate cybercrime and collect e-evidence in relation to **any** offence (articles 14-21)
   - Expedited preservation, production orders, search and seizure, interception, safeguards
3. International cooperation on cybercrime **and** e-evidence
   - General provisions, expedited preservation, MLA, 24/7 network

Second Protocol on enhanced cooperation and disclosure of e-evidence (2022):

- Scope: criminal investigations and proceedings related to computer systems and data and collection of e-evidence re **any** criminal offence
- Direct cooperation with service providers and registrars in other Parties
- Giving effect to production orders from other Parties
- Expedited cooperation in emergencies
- Video conferencing
- Joint investigation teams and joint investigations
- Data protection and other safeguards

Cybercrime & e-evidence!!!

8

1. About cybercrime treaties: Structure and scope of the proposed UN treaty

Structure of the current draft text of a convention on [cybercrime / use of information and communication technologies for criminal purposes]

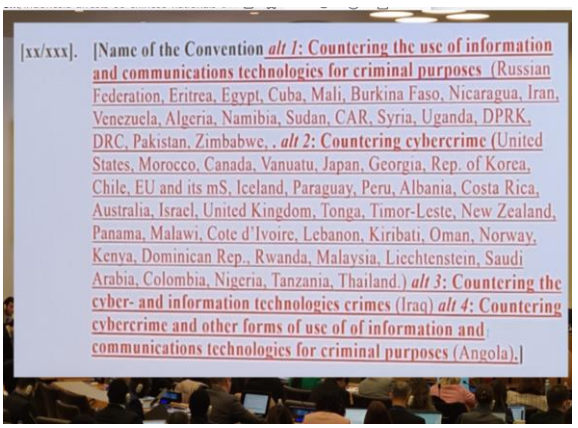
- Chapter I: General provisions (Scope: cybercrime [and electronic evidence])
- Chapter II: Criminalisation (copy/paste Budapest Convention + grooming + NCDII + money laundering + Art .17)
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement (copy/paste BC + seizing and confiscating assets)
- Chapter V: International cooperation (copy/paste UNTOC/UNCAC/BC + seizing and confiscating assets)
- Chapters VI - IX: Preventive measures, Technical assistance, Mechanism of implementation, Final provisions

9

1. About cybercrime treaties: UN treaty – status and issues

Draft text of the Convention – main issues:

- Terms/definitions:
  - Title
  - Article 2. Definitions
- Safeguards
  - Article 5. Respect for human rights
  - Article 24. Conditions and safeguards
  - Article 40. Grounds for refusal (political offences) and non-discrimination
- Scope
  - Article 3. Scope of application
  - Article 17. Offences relating to other international treaties
  - [Additional offences proposed by Russia+]
  - Article 23. Scope of procedural measures
  - Article 35. General principles of international cooperation
  - Article 40. General principles and procedures relating to mutual legal assistance



10

Q & A

European Court of Human Rights: ”positive obligations”

- Governments have to provide for effective measures, including through criminal law, to protect individuals against interference with their human rights by others

= Not providing for effective measures may be considered a violation of human rights

- Applicable also to crime online and use of criminal law tools of the Budapest Convention (See ECtHR: K.U. v Finland 2008)

[Balance of State interests and individual human rights OR balancing different rights?]

2. Human rights considerations

Human rights and rule of law standards are global (ECHR, African Convention, Inter-American Convention, ICCPR)

Conditions and safeguards regarding:

- Criminalisation
- Procedural powers (cybercrime and e-evidence)
- International cooperation

Criminal law measures on cybercrime and e-evidence may interfere with fundamental rights.

An interference must:

- be prescribed by law (clear, precise, accessible, foreseeable, overseen by an independent body etc.)
- pursue a legitimate aim (rights or reputation of others, national security, public order etc.)
- be necessary and proportionate (pressing and substantial need, least restrictive means to achieve the stated aim, etc.)

\+ Impact of laws and measures on cybercrime and e-evidence on other rights (privacy, freedom of expression etc.)

13

2. Human rights considerations

Concern: Cybercrime laws increasingly used to address speech in broad and vague terms

- "Prescribed by law? Clear, precise, foreseeable? Necessary? Proportionate?

Examples:

- Any person who publishes information or data presented in a picture, text, symbol or any other form in a computer system knowing that such information or data is false, deceptive, misleading or inaccurate, and with intent to defame, threaten, abuse, insult, or otherwise deceive or mislead the public or councelling commission of an offence, commits an offence, and shall be punishable …
- Anyone who knowingly uses information and communication systems and networks in order to produce, spread, disseminate, send or write false news, false data, rumours, false or falsified documents or documents falsely attributed to others with the aim of infringing the rights of others or harming public safety or national defence or spreading terror among the population shall be punished by five years' imprisonment and a fine …
- Any person who Knowingly or intentionally sends a message or other matter by means of computer system or network that:
  (a) Is grossly offensive or phonographic or an indecent obscene or menacing character or causes any such message or matter to be so sent; or
  (b) He knows to be false, for the purpose of annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred, ill will or needless anxiety to another or caused such a message to be sent: commits an offence under this act …

14

2. Human rights considerations

CNN World Watch Listen Live TV Sign In

World / Africa

A Nigerian woman reviewed some tomato puree online. Now she faces jail

By Nimi Princewill, CNN

6 minute read · Updated 10:56 PM EDT, Wed March 27, 2024

Abuja, Nigeria (CNN) — A Nigerian woman who wrote an online review of a can of tomato puree is facing imprisonment after its manufacturer accused her of making a "malicious allegation" that damaged its business.

Chioma Okoli, a 39-year-old entrepreneur from Lagos, is being prosecuted and sued in civil court for allegedly breaching the country's cybercrime laws, in a case that has gripped the West African nation and sparked protests by locals who believe she is being persecuted for exercising her right to free speech.

15

2. Human rights considerations

Octopus Project

www.coe.int/cybercrime

Link

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Considerations (examples):

- For legislators
  - The three-tier test of legality, proportionality and necessity is the key safeguard against excessive restrictions to the freedom of expression.
- For policy makers
  - Public figures shall be required to tolerate a greater degree of criticism.
  - Consider multistakeholder approach to combating disinformation.
- For criminal justice practitioners
  - Criminal law needs to be used as a last resort for addressing both disinformation and defamation.

16

2. Human rights considerations

Q & A

17

3. Budapest Convention on Cybercrime: Conditions and safeguards

Budapest Convention

- General: Link to human rights and specific COE and UN human rights treaties, incl. on data protection (Preamble)
- Criminalisation:
  - Limited list of offences against and by means of computers
  - Declarations and reservations
- Procedural powers on cybercrime and e-evidence of any crime:
  - Article 15 conditions and safeguards
    - Obligations pursuant to international HR treaties, principle of proportionality
    - Judicial or other supervision, grounds justifying application, limitation of scope and duration
  - Specified data needed in specific criminal investigations
- International cooperation
  - Broad cooperation
  - Grounds for refusal
  - Confidentiality and use limitation

18

3. Budapest Convention on Cybercrime: Conditions and safeguards

Second Protocol on e-evidence

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

19

3. Budapest Convention on Cybercrime: Conditions and safeguards

Q & A

20

Recap 1. About cybercrime treaties: UN treaty – status and issues

Structure of the revised draft text of a convention on [cybercrime / use of information and communication technologies for criminal purposes] *

- Chapter I: General provisions (Scope: cybercrime [and electronic evidence])
- Chapter II: Criminalisation (copy/paste Budapest Convention + grooming + NCDII + money laundering + Art .17)
- Chapter III: Jurisdiction
- Chapter IV: Procedural measures and law enforcement (copy/paste BC + seizing and confiscating assets)
- Chapter V: International cooperation (copy/paste UNTOC/UNCAC/BC + seizing and confiscating assets)
- Chapters VI - IX: Preventive measures, Technical assistance, Mechanism of implementation, Final provisions

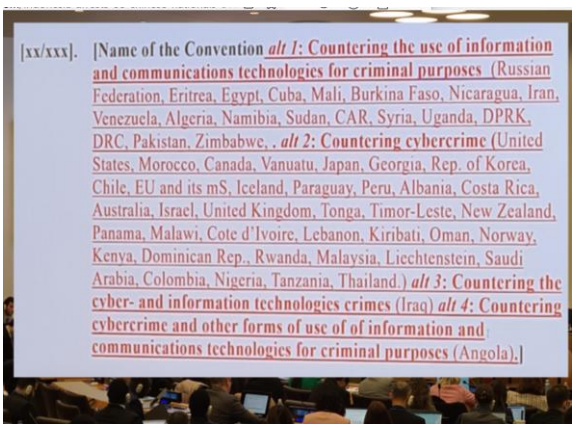
* "Zero draft" discussed by AHC 6 (Aug/Sep 2023) / Revised draft text under discussion by AHC 7 (Jan/Feb 2024)

21

Recap 1. About cybercrime treaties: UN treaty – status and issues

Draft text of the Convention – main issues:

- Terms/definitions:
  - Title
  - Article 2. Definitions
- Safeguards
  - Article 5. Respect for human rights
  - Article 24. Conditions and safeguards
  - Article 40. Grounds for refusal (political offences) and non-discrimination
- Scope
  - Article 3. Scope of application
  - Article 17. Offences relating to other international treaties
  - [Additional offences proposed by Russia+]
  - Article 23. Scope of procedural measures
  - Article 35. General principles of international cooperation
  - Article 40. General principles and procedures relating to mutual legal assistance



22

4. UN draft treaty: Human rights and rule of law risks and solutions

Human rights and rule of law risks:

- Treaty may "permit or facilitate repression or suppression of political activity, expression, conscience, opinion, belief, assembly or association; or permit or facilitate discrimination or persecution based on personal characteristics"
- Definitions and concepts: cybercrime v. "information crime"
- Criminalisation: overbroad list and scope of offences
- Domestic investigations and prosecution:
  - Misuse of intrusive procedural powers
  - Freezing and confiscating property/assets to target individuals, civil society, businesses, service providers etc.
- International cooperation: Parties may be obligated to cooperate even in cases where HR are violated.
- Free, open and global internet with multi-stakeholder governance v. sovereign, government-controlled cyberspace

23

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: Treaty to facilitate or permit repression of rights

Solution TBC:

- Keep or further strengthen Article 5. Respect for human rights
  "States Parties shall ensure that the implementation of their obligations under this Convention is consistent with their obligations under international human rights law."
- "Canadian" addition to Article 3. Scope):
  "Nothing in this Convention or its interpretation or application by States shall permit or facilitate repression or suppression of political activity, expression, conscience, opinion, belief, assembly or association; or permit or facilitate discrimination or persecution based on personal characteristics".

24

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: Terminology and underlying concepts ["information crime"]

- [Cybercrime] [Use of ICT for criminal purposes]
- [Computer system] [Information and communications technology device]
- [Computer data] [Digital information]

= Cybercrime or "Information crime?"

Solution TBC:

- Make use of proven terminology and concepts of the Budapest Convention

25

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: Criminalisation

- Article 16 – Money laundering
- Article 17 – Open-ended criminalisation
- Russian additions on extremism, terrorism etc.
- Criminalisation of dissent (information crime)

NOTE: Some States wish to commence the negotiation of Protocols without delay.

Solutions TBC:

- Limit the list and scope of offences
- Delete or narrow article 16
- Delete (or narrow) article 17
- Or limit procedural law and international cooperation to articles 6 to 15/16 and serious crime
- Respect for human rights article 5
- "Canadian" addition to scope (article 3): Nothing in this convention shall be used to suppress political activity etc.

26

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: Targeting assets as a means to suppress dissent and fundamental rights

- Article 16 – Money laundering
- Article 31 – Freezing, seizure and confiscation of the proceeds of crime
- Article 49 – International cooperation for the recovery of confiscated assets
- Etc.

Solutions TBC:

- Delete or narrow article 16
- Limit scope of articles on money laundering and seizure and confiscation to offences of Articles 6 to 15 [but problem of broad fraud provisions remains]
- Canadian addition to article 3

27

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: Misuse of procedural powers

Articles

- 25. Expedited preservation
- 26. Preservation and partial disclosure
- 27. Production orders
- 28. Search and seizure
- 29. Real-time collection of traffic data
- 30. Interception of content data
- 31. Freezing, seizure and confiscation of the proceeds of crime

Solutions TBC:

- Strengthen Article 24 on conditions and safeguards (align with Article 15 BC)

28

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: International cooperation

- Parties may be obligated to cooperate, provide information/evidence or extradite persons even in cases where human rights are violated in the requesting Party.
- Risks to the protection of personal data

Solutions TBC:

- 35. General principles of international cooperation
  - ► Limit cooperation to offences under articles 6 to 15 (or 16) and electronic evidence of serious crime
- 36. Protection of personal data
  - ► Keep or improve further.
- 40. General principles of mutual legal assistance
  - ► Add "political offences" as ground for refusal
  - ► Add non-discrimination provision of article 37.15 to article 40

29

4. UN draft treaty: Human rights and rule of law risks and solutions

Risk: International cooperation

- Free, open and global internet with multi-stakeholder governance v. sovereign, government-controlled cyberspace

Solutions TBC:

- States and stakeholders to remain engaged in the process
- Seek agreement by consensus or broad support (2/3)

30

4. UN draft treaty: Human rights and rule of law risks and solutions

Status as of 23 April 2024

From 67 articles:

- 19 articles agreed “ad referendum”
- 30 articles partially agreed
- 18 articles not agreed (scope, human rights, CSAM, interception, international cooperation)

	Preamble	
	Article 1	Paragraphs (a) and (b)
	Article 2	Paragraph 1 (d)
	Article 3	
	Article 4	
	Article 5	
	Article 6	Paragraph 1
	Article 7	Paragraph 1
	Article 8	Paragraph 2
	Article 9	Entire article
	Article 10	Entire article
	Article 11	Paragraph 1
	Article 12	Chapeau and subparagraphs (b) and (
	Article 13	
	Article 14	Entire article
	Article 15	
	Article 16	Paragraph 1; paragraph 2 (d) to (g)
	Article 17	
	Article 18	Entire article
	Article 19	Entire article
	Article 20	Entire article
	Article 21	Paragraphs 1, 3 and 5 to 8
	Article 22	Paragraph 1; paragraph 2 (chapeau) a paragraphs 3 to 6
	Article 23	
	Article 24	
	Article 25	Entire article
	Article 26	Entire article
	Article 27	Entire article
	Article 28	Entire article
	Article 29	
	Article 30	
	Article 31	Entire article
	Article 32	Entire article
	Article 33	Entire article
	Article 34	Paragraphs 1 to 3
	Article 35	
	Article 36	
	Article 37	Paragraphs 1 to 3, 5 to 14, 16, 17, and 20
	Article 38	
	Article 39	Paragraph 2
	Article 40	
	Article 41	Paragraph 4
	Article 42	Paragraph 3, subparagraphs (a), (c) to (g); paragraph 4
	Article 43	Paragraph 1
	Article 44	Paragraphs 2 and 3
	Article 45	
	Article 46	
	Article 47	Paragraph 1, subparagraphs (b) to (e)
	Article 48	
	Article 49	Paragraph 1, subparagraphs (b) and (c); paragraph 2
	Article 50	Paragraph 1, subparagraph (a); paragraphs 3 to 6 and 8 to 10
	Article 51	
	Article 52	Paragraphs 1 and 2
	Article 53	Paragraph 1; Paragraph 3, subparagraphs (b), (c), (f), (j), (k); paragraph
	Article 54	Paragraph 3 (chapeau) and subparagraphs (b) to (f), (h) and (i); paragraphs 7, and 9
	Article 55	Paragraph 4

31

4. UN draft treaty: Human rights and rule of law risks and solutions

Submission by the Russian Federation (15 April 2024)

Concept Note on the Human Rights Provisions of the Draft Convention on Countering the Use of Information and Communications Technologies (ICT) for Criminal Purposes

.....

Excessive attention to human rights provisions in the Convention is significantly detrimental to international cooperation and will in fact hinder the cooperation between law enforcement agencies of states parties. The Russian experience of cooperation with Western countries on various regional platforms (including European ones) proves that this issue is used to promote opportunistic interests and politicise discussions.

.....

32

5. Conclusions

- UN treaty:
  - A treaty with the above solutions may be an acceptable outcome for the majority of States.
  - Without strong safeguards, many States (including those with which cooperation is essential) will not be able sign and ratify.

AHC 7 (29 Jan-9 Feb 2024):

- "Concluding session" not conclusive …

AHC 7bis (29 July – 9 Aug 2024 TBC):

- Ensure that agreement on an acceptable treaty can be achieved.
- But be also prepared for a no-consensus scenario.

- Budapest Convention framework:
  - The number of Parties will increase whether or not there will be an additional UN treaty.
  - Full implementation of the provisions of the Convention and its Protocols – including safeguards – is a condition for joining.
  - More focus on impact of cybercrime laws on freedom of expression.
  - More capacity building by C-PROC.

33

5. Conclusions

Q & A