Cybercrime: Fundamentals and the need for international cooperation

Alexander Seger

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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

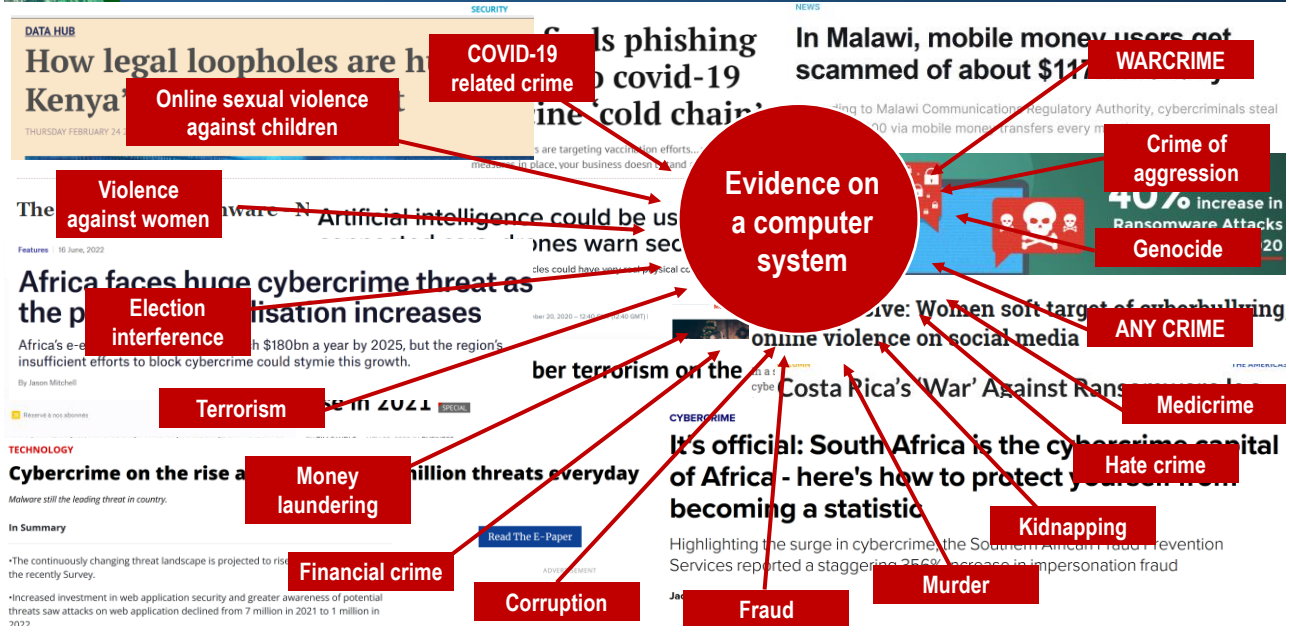
Fundamentals

- Cybercrime requires a criminal justice response that is:
  - effective
  - meets human rights and rule of law requirements
- Comprehensive cybercrime legislation is the basis:
  - establish offences against and by means of computers
  - powers for criminal justice authorities to investigate and prosecute cybercrime and secure electronic evidence
  - permit international cooperation
- International cooperation on cybercrime and electronic evidence essential:
  - make use of frameworks such as the Budapest Convention
  - develop trusted partnerships
- Capacity building:
  - define reforms / processes of change to be supported

The problem of cybercrime …

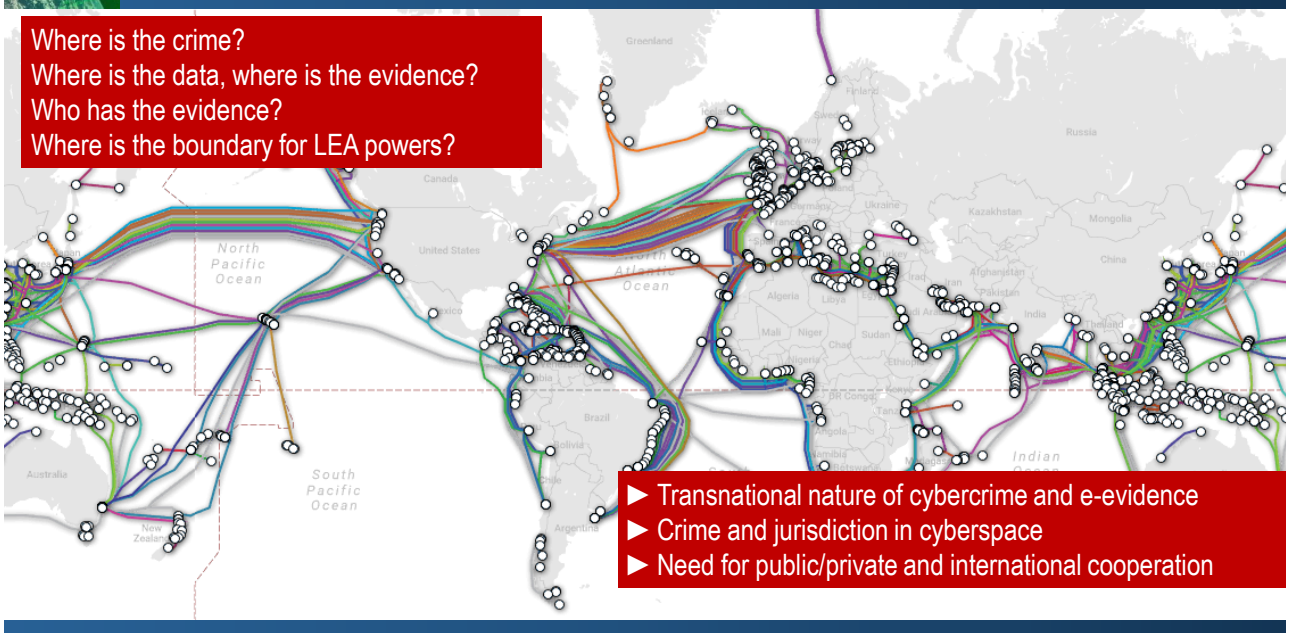
Cybercrime:
Offences against and by means of computers

… and e-evidence re all types of crime



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?



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

The mechanism of the Convention on Cybercrime

Budapest Convention on Cybercrime (2001):

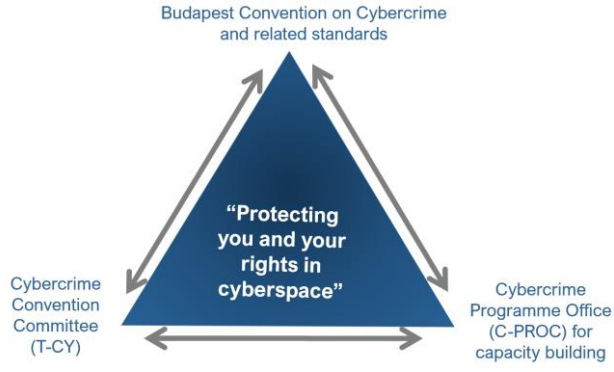
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

+ Guidance Notes

+ 2nd Protocol on enhanced cooperation and disclosure of electronic evidence (opened for signature 12 May 2022)

By July 2023: **68 Parties and 21 Observer States**



Content of the 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
- 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

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

Content of the First Protocol on xenophobia and racism

ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME, CONCERNING THE CRIMINALISATION OF ACTS OF A RACIST AND XENOPHOBIC NATURE COMMITTED THROUGH COMPUTER SYSTEMS (ETS 189)

Article 2: Definition

"*racist and xenophobic material*" means any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.

- Article 3 – Dissemination of racist and xenophobic material through computer systems.
- Article 4 – Racist and xenophobic motivated threat
- Article 5 – Racist and xenophobic motivated insult
- Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity…
- Article 7 – Aiding and abetting

Content of the Second Protocol on e-evidence

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

Content of the Budapest Convention: example ransomware ► Guidance Note

Article	Budapest Convention on Cybercrime
Art. 2	Illegal access
Art. 3	Illegal interception
Art. 4	Data interference
Art. 5	System interference
Art. 6	Misuse of devices
Art. 7	Computer-related forgery
Art. 8	Computer-related fraud
Art. 11	Attempt, aiding, abetting
Art. 12	Corporate liability
Art. 13	Sanctions and measures

Article	Convention on Cybercrime
Art. 14-21	Procedural powers

Ransom-ware offences

Article	Convention on Cybercrime
Art. 23-35	International cooperation

Article	2nd Additional Protocol to Convention on Cybercrime
Art. 7	(Direct) Disclosure of subscriber information
Art. 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data
Art. 9	Expedited disclosure of stored computer data in an emergency
Art. 10	Emergency mutual assistance
Art. 11	Video conferencing
Art. 12	Joint investigation teams and joint investigations

The Convention on Cybercrime: Backed up by capacity building

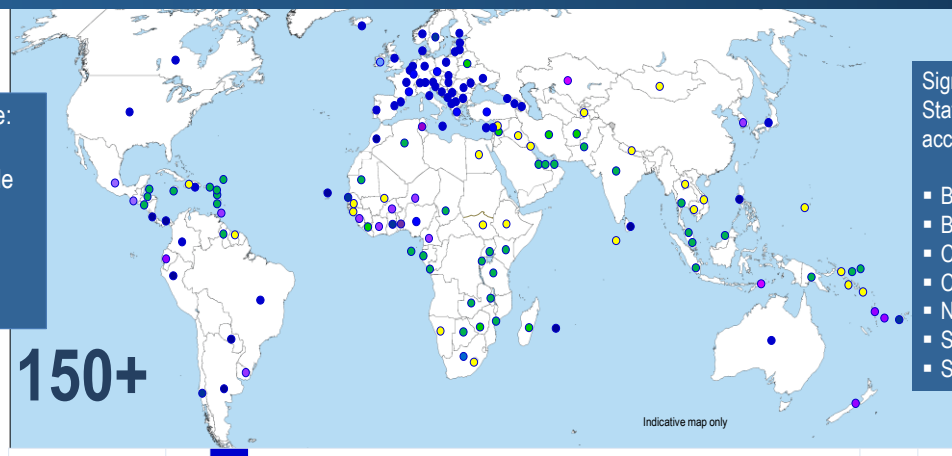
Cybercrime Programme Office of the Council of Europe (C-PROC) in Romania:

- Support processes of change towards stronger criminal justice capacities on cybercrime and e-evidence in line with the Budapest Convention and with rule of law safeguards
- 5 ongoing projects with a cumulative budget of EUR 40 million
- 40 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Italy, Japan, Netherlands, UK and USA in 2022/23
- Support to T-CY

Current projects:

- GLACY+
- CyberEast
- CyberSouth
- iPROCEEDS-2
- Octopus

Reach of the Convention on Cybercrime



Parties include:

- Cabo Verde
- Ghana
- Mauritius
- Nigeria
- Senegal

Signatories and States invited to accede include:

- Benin
- Burkina Faso
- Cameroun
- Côte d'Ivoire
- Niger
- Sierra Leone
- South Africa

Parties:	68			
Signed:	2	Other States with substantive laws broadly in line with Budapest Convention:	40+	
Invited to accede:	19	Further States drawing on Budapest Convention for legislation:	30+	
=	**89**	=	**70+**	

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Phase 1:
- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:
- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

For any query contact:
Alexander.seger@coe.int
Executive Secretary
Cybercrime Convention Committee
Council of Europe

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Will the State requesting accession have legislation in line with the Convention by the time of accession?
- Rule of law safeguards of Article 15: conditions and safeguards for coercive powers?
- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?
  - Risk of capital punishment as a result of cooperation under the Convention?

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Rule of law safeguards of Article 15: conditions and safeguards for coercive powers?

Article 15 – Conditions and safeguards
1. Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality.

2. Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, *inter alia*, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure.

3. To the extent that it is consistent with the public interest …

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?

African Charter on Human and Peoples' Rights (ACHPR)

Article 1

"The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Charter and shall undertake to adopt legislative or other measures to give effect to them."

Article 9

1. *Every individual shall have the right to receive information.*
2. *Every individual shall have the right to express and disseminate his opinions within the law.*

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?

African Charter on Human and Peoples' Rights (ACHPR)

Article 1

"The Member States of the Organization of African Unity parties to the present Charter shall recognize the rights, duties and freedoms enshrined in this Charter and shall undertake to adopt legislative or other measures to give effect to them."

Article 9

1. Every individual shall have the right to receive information.
2. Every individual shall have the right to express and disseminate his opinions within the law.

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa**,
(adopted at its 65th Ordinary Session, held from 21 October to 10 November 2019, in Banjul, Gambia)

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)**

Principle 9 ► conditions for a justifiable limitation of the exercise of the right to freedom of expression and access to information

"1.States may only limit the exercise of the, if the limitation:
- a. is prescribed by law;
- b. serve a legitimate aim; and
- c. is a necessary and proportionate means to achieve the stated aim in a democratic society.

2. States shall ensure that any law limiting the rights to freedom of expression and access to information:
- a. is clear, precise, accessible and foreseeable;
- b. is overseen by an independent body …
- c. effectively safeguards against abuse …

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa** (2019)

Principle 9 ► conditions for a justifiable limitation of the exercise of the right to freedom of expression and access to information

3. A limitation shall serves a **legitimate aim** where the objective of the limitation is:

a. to preserve respect for the rights or reputations of others; or
b. to protect national security, public order or public health.

4. To be **necessary and proportionate**, the limitation shall:

a. originate from a pressing and substantial need that is relevant and sufficient
b. have a direct and immediate connection to the expression and disclosure of information, and be the least restrictive means of achieving the stated aim; …

How to accede to the Convention on Cybercrime

Treaty open for accession (article 37)

Considerations:

- Human rights:
  - Do (cybercrime) laws interfere with fundamental rights (such as privacy or freedom of expression) beyond what is necessary/proportionate?

► African Commission: **Declaration of Principles of Freedom of Expression and Access to Information in Africa (2019)**

Principle 21 ► Protecting reputations

"1.States shall ensure that laws relating to defamation in accordance with the following
standards:

a. No one shall be found liable for true statements, expressions of opinions or statements which are reasonable to make in the circumstances.
b. Public figures shall be required to tolerate a greater degree of criticism.
c. Sanctions shall never be so severe as to inhibit the right to freedom of expression.

2. Privacy and secrecy laws shall not inhibit the dissemination of information of public interest."

How to accede to the Convention on Cybercrime

Starting point:

Domestic legislation on cybercrime and electronic evidence

The Budapest Convention and domestic legislation: examples

Budapest Convention
Article 3 – Illegal interception

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Tanzania - Cybercrimes Act 2015
Illegal interception

6.-(1) A person shall not intentionally and unlawfully- (a) intercept by technical means or by any other means- (i) a non-public transmission to, from or within a computer system; (ii) a non-public electromagnetic emission from a computer system; (iii) a non-public computer system that is connected to another computer system; or (b) circumvent the protection measures implemented to prevent access to the content of non-public transmission.
(2) A person who contravenes subsection (1) commits an offence and is liable, on conviction, to a fine of not less than five million shillings or to imprisonment for a term of not less than one year or to both.

The Budapest Convention and domestic legislation: examples

Budapest Convention

Article 4 – Data interference

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

Mozambique

Codigo Penal (Lei n.º 24/2019)

ARTIGO 337 - (Interferência em dados)

1. Quem alterar, deteriorar, inutilizar, apagar, suprimir, destruir ou, de qualquer forma, alterar dados informáticos, é punido com a pena de prisão de 1 a 2 anos e multa correspondente.
2. A mesma pena é aplicável a quem, mediante a introdução ou transmissão de dados informáticos ou, por qualquer outra forma, instalando vulnerabilidades, interferir no funcionamento de sistema informático, causando intencionalmente dano a alguém.

The Budapest Convention and domestic legislation: examples

Budapest Convention

Article 8 – Computer-related fraud

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
a any input, alteration, deletion or suppression of computer data;
b any interference with the functioning of a computer system,
with fraudulent or dishonest intent of procuring,

Kenya - THE COMPUTER MISUSE AND CYBERCRIMES ACT No. 5 of 2018 (CMCA)

Article 26. Computer fraud
(1) A person who, with fraudulent or dishonest intent—
(a) unlawfully gains;
(b) occasions unlawful loss to another person; or
(c) obtains an economic benefit for oneself or for another person, through any of the means described in subsection (2),

commits an offence and is liable, on conviction, to a fine not exceeding twenty million shillings or imprisonment term for a term not exceeding ten years, or to both.
….

The Budapest Convention and domestic legislation: examples

Budapest Convention

Article 16 – Expedited preservation of stored computer data

1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

…..

Tanzania - Cybercrimes Act 2015
Expedited preservation
33.-(1) Where there is a reasonable ground to believe that a computer data that is required for the purpose of investigation is vulnerable to loss or modification, the police officer incharge of a police station or a law enforcement officer of a similar rank may issue an order requiring the person in control of a device or computer data to preserve the device or computer data for a period not exceeding fourteen days. (2) The court may, on application, extend the order made under section 35 for such period as the court may deem necessary

The Budapest Convention and domestic legislation: examples

Budapest Convention
Article 9 – Offences related to child pornography
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:
a producing child pornography for the purpose of its distribution through a computer system;
b offering or making available child pornography through a computer system;
c distributing or transmitting child pornography through a computer system;
d procuring child pornography through a computer system for oneself or for another person;
e possessing child pornography in a computer system or on a computer-data storage medium.
……

Malawi - Electronic Transactions and Cyber Security Act 2016 (No. 33 of 2016)
Article 85- Child pornography
(1) Child pornography in an electronic form is prohibited under this Act.
(2) Any person who:
(a) produces pornographic material for the purpose of its distribution through a computer system;
(b) reproduces pornographic material for the purpose of its distribution through an information system;
(c) offers or makes available any pornographic material through an information system;
(d) exposes a child to pornographic material through an information system;
(e) distributes or transmits any pornographic material through an information system;
(f) procures any pornographic material through a computer system for oneself or for another person; or
(g) possesses any child pornographic material in a computer system or on a computer data storage medium, commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and to imprisonment for fifteen years.
….

The Budapest Convention and domestic legislation

Domestic legislation and accession to the Budapest Convention:

What is the current status in

- Kenya
- Malawi
- Mozambique
- Tanzania

?

Fundamentals

- Cybercrime requires a criminal justice response that is:
  - effective
  - meets human rights and rule of law requirements
- Comprehensive cybercrime legislation is the basis:
  - establish offences against and by means of computers
  - powers for criminal justice authorities to investigate and prosecute cybercrime and secure electronic evidence
  - permit international cooperation
- International cooperation on cybercrime and electronic evidence essential:
  - make use of frameworks such as the Budapest Convention
  - develop trusted partnerships
- Capacity building:
  - define reforms / processes of change to be supported