Conference on xenophobia and racism committed through computer systems
Strasbourg, France, 30-31 January 2023
20th Anniversary of the first Protocol to the Convention on Cybercrime

Session 2: Good practices and challenges in implementing the First Additional Protocol to the Convention on Cybercrime

The Convention on Cybercrime and its Protocols:

a framework for addressing xenophobia and racism via computer systems

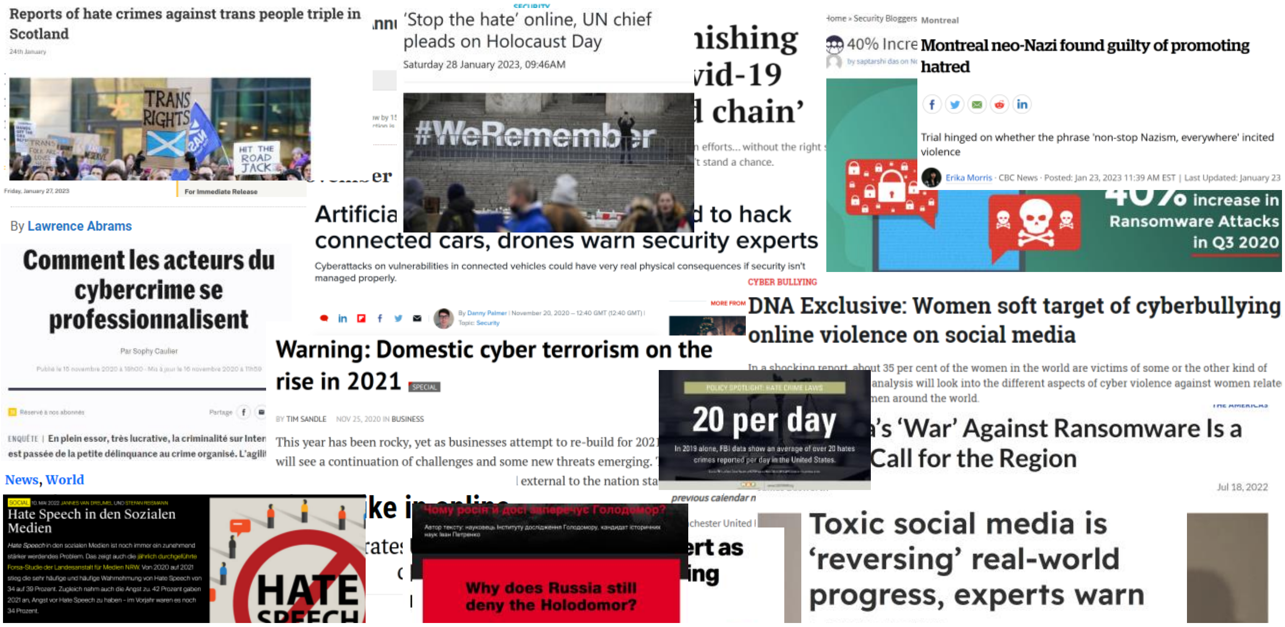
Alexander Seger

Head of Cybercrime Division
Council of Europe

www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

The problem of cybercrime …



Reports of hate crimes against trans people triple in Scotland

24th January

Friday, January 27, 2023

For Immediate Release

By Lawrence Abrams

Comment les acteurs du cybercrime se professionnalisent

Par Sophy Caulier

Publié le 15 novembre 2020 à 19h00 - Mis à jour le 16 novembre 2020 à 11h59

Réservé à nos abonnés

Partage

ENQUÊTE | En plein essor, très lucrative, la criminalité sur Inter
est passée de la petite délinquance au crime organisé. L'agili

News, World

SOCIAL 10. MAI 2022 JANNES VAN DREUMEL UND STEFAN REISMANN

Hate Speech in den Sozialen Medien

Hate Speech in den sozialen Medien ist noch immer ein zunehmend stärker werdendes Problem. Das zeigt auch die jährlich durchgeführte Forsa-Studie der Landesanstalt für Medien NRW. Von 2020 auf 2021 stieg die sehr häufige und häufige Wahrnehmung von Hate Speech von 34 auf 39 Prozent. Zugleich nahm auch die Angst zu. 42 Prozent gaben 2021 an, Angst vor Hate Speech zu haben – im Vorjahr waren es noch 34 Prozent.

SECURITY

'Stop the hate' online, UN chief pleads on Holocaust Day

Saturday 28 January 2023, 09:46AM

Artificia… connected cars, drones warn security experts

Cyberattacks on vulnerabilities in connected vehicles could have very real physical consequences if security isn't managed properly.

By Danny Palmer | November 20, 2020 – 12:40 GMT (12:40 GMT) |
Topic: Security

…ishing …vid-19 …l chain'

…n efforts... without the right … …'t stand a chance.

…d to hack

Warning: Domestic cyber terrorism on the rise in 2021 SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

This year has been rocky, yet as businesses attempt to re-build for 2021 … will see a continuation of challenges and some new threats emerging. … external to the nation sta…

Чому росія й досі заперечує Голодомор?

Автор тексту: науковець Інституту дослідження Голодомору, кандидат історичних наук Іван Петренко

Why does Russia still deny the Holodomor?

Home » Security Bloggers

40% Incre…

by saptarshi das on N…

40% increase in Ransomware Attacks in Q3 2020

Montreal

Montreal neo-Nazi found guilty of promoting hatred

Trial hinged on whether the phrase 'non-stop Nazism, everywhere' incited violence

Erika Morris · CBC News · Posted: Jan 23, 2023 11:39 AM EST | Last Updated: January 23

CYBER BULLYING

MORE FROM

DNA Exclusive: Women soft target of cyberbullying online violence on social media

In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of … analysis will look into the different aspects of cyber violence against women relate… …men around the world.

POLICY SPOTLIGHT: HATE CRIME LAWS

20 per day

In 2019 alone, FBI data show an average of over 20 hates crimes reported per day in the United States.

previous calendar n…

THE AMERICAS

…a's 'War' Against Ransomware Is a Call for the Region

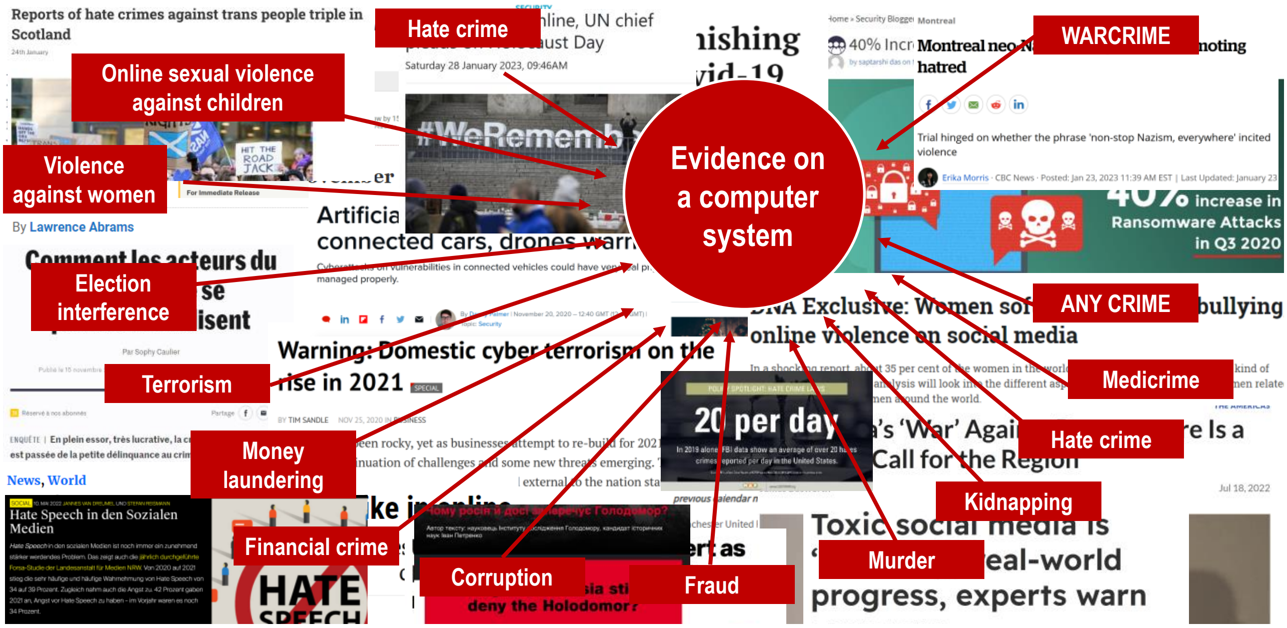
Jul 18, 2022

…chester United …

…ert as …ing

Toxic social media is 'reversing' real-world progress, experts warn

… and e-evidence re all types of crime



The mechanism of the Convention on Cybercrime

Budapest Convention on Cybercrime (2001):

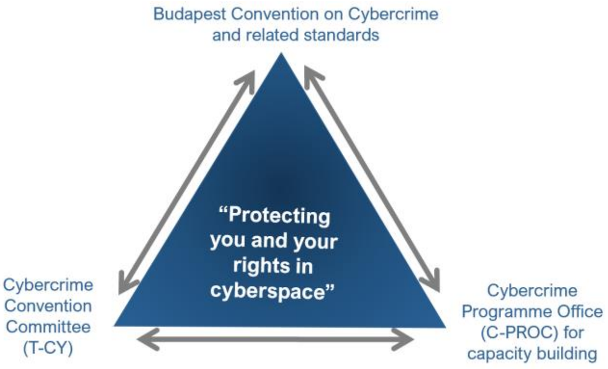
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

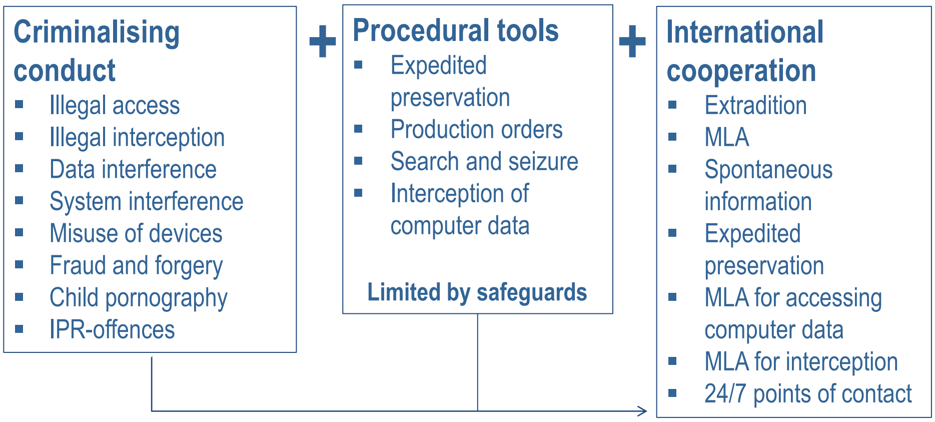
+ Guidance Notes

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

By 29 January 2022: **68 Parties and 15 Observer States**


Budapest Convention on Cybercrime and related standards
"Protecting you and your rights in cyberspace"
Cybercrime Convention Committee (T-CY)
Cybercrime Programme Office (C-PROC) for capacity building

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

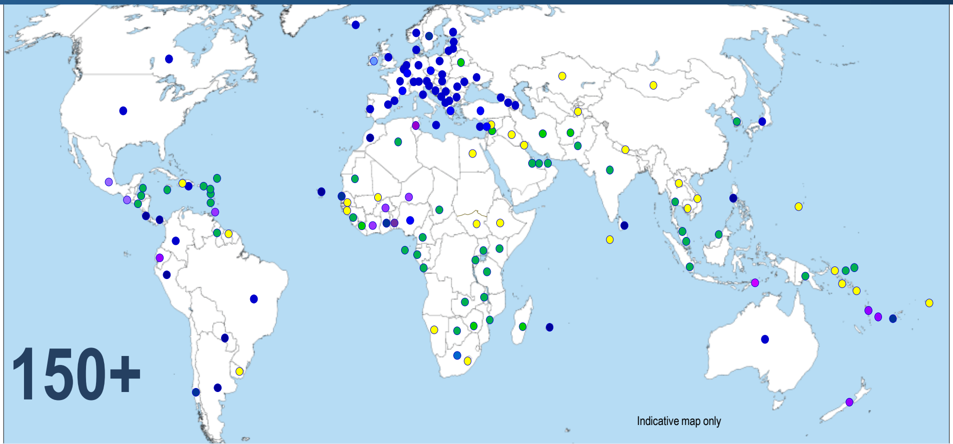
+

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!

Reach of the Convention on Cybercrime



150+

Parties:	68	🟦			
Signed:	2	🟦	Other States with substantive laws broadly in line with Budapest Convention:	45+	🟩
Invited to accede:	13	🟪	Further States drawing on Budapest Convention for legislation:	30+	🟨
=	**83**		=	**75+**	

The first Protocol on Xenophobia and Racism: about

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

Opened for signature on 28 January 2003

The first Protocol on Xenophobia and Racism: background

- Convention for the Protection of Human Rights and Fundamental Freedoms and its Protocol No. 12 concerning the general prohibition of discrimination
- United Nations International Convention on the Elimination of All Forms of Racial Discrimination of 21 December 1965 (177 Parties by June 2015)
- the European Union Joint Action of 15 July 1996 adopted by the Council on the basis of Article K.3 of the Treaty on European Union, concerning action to combat racism and xenophobia
- Council of Europe: European Commission against Racism and Intolerance, ECRI, established in 2002 (www.coe.int/ecri)
- The Internet offers new opportunities for acts of xenophobia and racism
- Acts of racism and xenophobia are crimes (not only if speech presents a "clear and present danger")

= Need for Protocol to Budapest Convention

The first Protocol on Xenophobia and Racism: background

Action Plan

The fight against violent extremism and radicalisation leading to terrorism

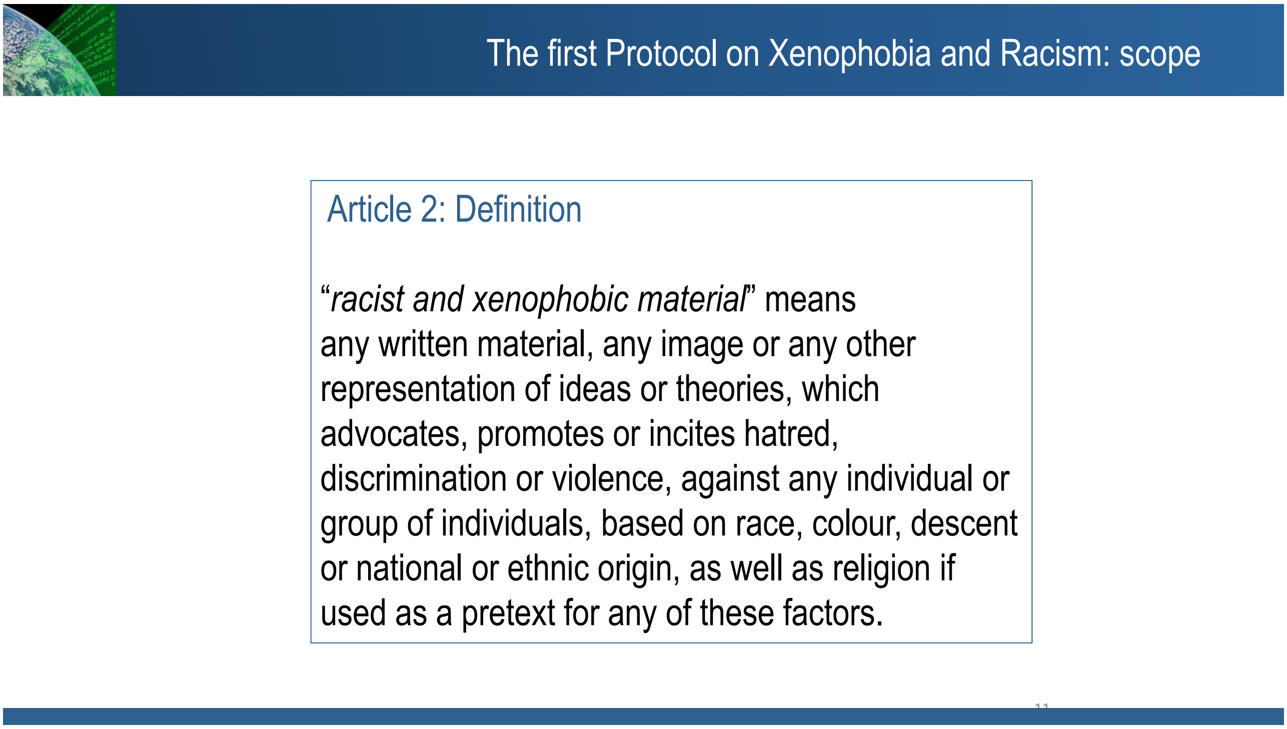
(Adopted by the Committee of Ministers, Brussels, 19 May 2015)

- ► Reinforcing international legal framework against terrorism and violent extremism, including implementation of:
  - Convention on the Prevention of Terrorism
  - Additional Protocol on Foreign Terrorist Fighters
  - **Protocol to Budapest Convention on Xenophobia and Racism**
- ► Education
- ► Addressing radicalisation in prisons
- ► Internet: No Hate Speech

The first Protocol on Xenophobia and Racism: purpose

Protocol XR – Preamble

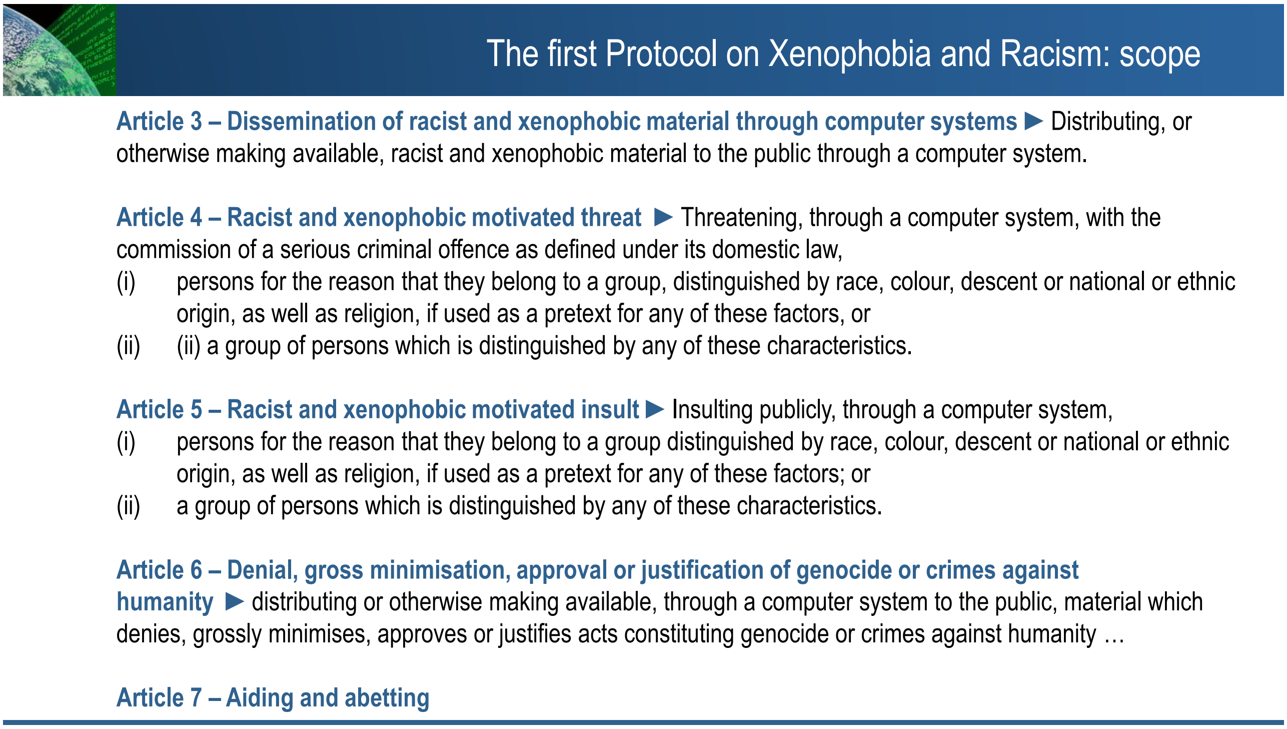
- Need to secure a full and effective implementation of all human rights without any discrimination or distinction;
- **Acts of a racist and xenophobic nature constitute a violation of human rights and a threat to the rule of law and democratic stability**;
- Computer systems offer an unprecedented means of facilitating freedom of expression and communication around the globe;
- **Risk of misuse or abuse of computer systems** to disseminate racist and xenophobic propaganda;
- Need to ensure a **proper balance between freedom of expression and an effective fight against acts of a racist and xenophobic nature**;
- This Protocol is not intended to affect established principles relating to freedom of expression in national legal systems.



The first Protocol on Xenophobia and Racism: scope

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.



The first Protocol on Xenophobia and Racism: scope

Article 3 – Dissemination of racist and xenophobic material through computer systems ▶ Distributing, or otherwise making available, racist and xenophobic material to the public through a computer system.

Article 4 – Racist and xenophobic motivated threat ▶ Threatening, through a computer system, with the commission of a serious criminal offence as defined under its domestic law,

(i) persons for the reason that they belong to a group, distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors, or

(ii) (ii) a group of persons which is distinguished by any of these characteristics.

Article 5 – Racist and xenophobic motivated insult ▶ Insulting publicly, through a computer system,

(i) persons for the reason that they belong to a group distinguished by race, colour, descent or national or ethnic origin, as well as religion, if used as a pretext for any of these factors; or

(ii) a group of persons which is distinguished by any of these characteristics.

Article 6 – Denial, gross minimisation, approval or justification of genocide or crimes against humanity ▶ distributing or otherwise making available, through a computer system to the public, material which denies, grossly minimises, approves or justifies acts constituting genocide or crimes against humanity …

Article 7 – Aiding and abetting

The first Protocol on Xenophobia and Racism: implementation

Parties

- Albania
- Andorra
- Armenia
- Bosnia and Herzegovina
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Finland
- France
- Germany
- Greece
- Latvia
- Lithuania
- Luxembourg
- Moldova
- Monaco
- Morocco
- Montenegro
- Netherlands
- North Macedonia
- Norway
- Paraguay
- Poland
- Portugal
- Romania
- San Marino
- Senegal
- Serbia
- Slovenia
- Spain
- Sweden
- Ukraine

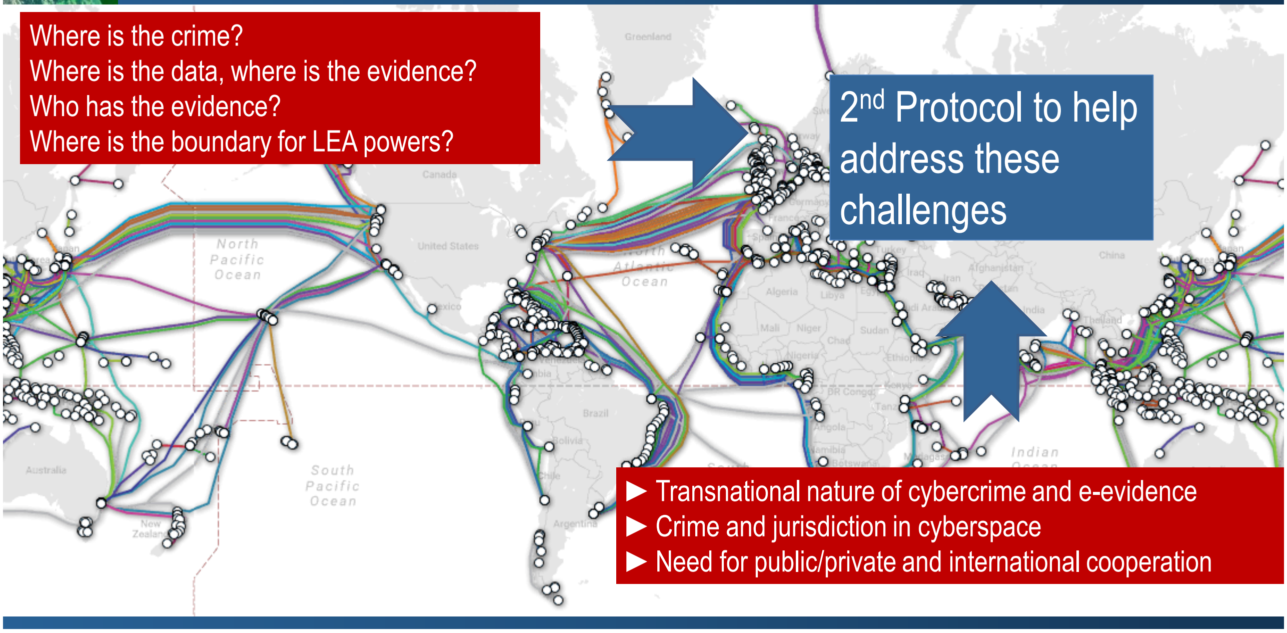
Signatories

- Canada
- Austria
- Belgium
- Estonia
- Iceland
- Italy
- Liechtenstein
- Malta
- Slovakia
- Switzerland
- South Africa
- Türkiye

Status as at 28 January 2023

▶ 33 Parties + 12 Signatories

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?

2nd Protocol to help address these challenges

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

2nd Additional Protocol to the Convention on Cybercrime: content

Preamble

Chapter I: Common provisions

Article 1	Purpose
Article 2	Scope of application
Article 3	Definitions
Article 4	Language

Chapter II: Measures for enhanced cooperation

Article 5	General principles applicable to Chapter II
Article 6	Request for domain name registration information
Article 7	Disclosure of subscriber information
Article 8	Giving effect to orders from another party for expedited production of subscriber information and traffic data
Article 9	Expedited disclosure of stored computer data in an emergency
Article 10	Emergency mutual assistance
Article 11	Video conferencing
Article 12	Joint investigation teams and joint investigations

Chapter III – Conditions and safeguards

Article 13	Conditions and safeguards
Article 14	Protection of personal data

Chapter IV: Final provisions

Article 15	Effects of this Protocol
Article 16	Signature and entry into force
Article 17	Federal clause
Article 18	Territorial application
Article 19	Reservations and declarations
Article 20	Status and withdrawal of reservations
Article 21	Amendments
Article 22	Settlement of disputes
Article 23	Consultations of the Parties and assessment of implementation
Article 24	Denunciation
Article 25	Notification

2nd Additional Protocol to the Convention on Cybercrime: next

2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence (CETS 224)

Signatories (status 29 January 2023):

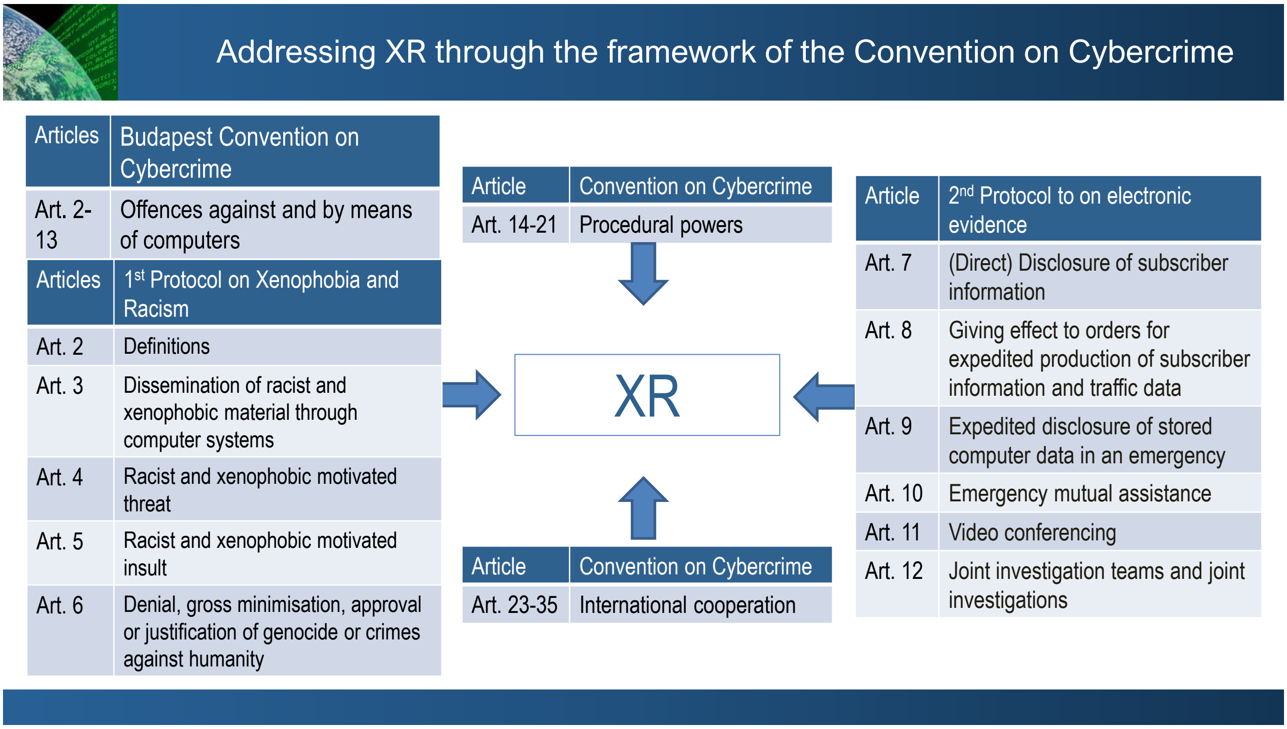
1. Andorra
2. Austria
3. Belgium
4. Bulgaria
5. Chile
6. Colombia
7. Costa Rica
8. Croatia
9. Estonia
10. Finland
11. France
12. Germany
13. Greece
14. Iceland
15. Italy
16. Japan
17. Lithuania
18. Luxembourg
19. Montenegro
20. Moldova
21. Morocco
22. Netherlands
23. North Macedonia
24. Portugal
25. Romania
26. Serbia
27. Slovenia
28. Spain
29. Sri Lanka
30. Sweden
31. Ukraine
32. United Kingdom
33. USA

Next:

▶ Signature by other Parties

▶ Ratification (5 needed for entry into force)

▶ Capacity building



Addressing XR through the framework of the Convention on Cybercrime

Articles	Budapest Convention on Cybercrime
Art. 2-13	Offences against and by means of computers

Articles	1st Protocol on Xenophobia and Racism
Art. 2	Definitions
Art. 3	Dissemination of racist and xenophobic material through computer systems
Art. 4	Racist and xenophobic motivated threat
Art. 5	Racist and xenophobic motivated insult
Art. 6	Denial, gross minimisation, approval or justification of genocide or crimes against humanity

Article	Convention on Cybercrime
Art. 14-21	Procedural powers

XR

Article	Convention on Cybercrime
Art. 23-35	International cooperation

Article	2nd Protocol to on electronic evidence
Art. 7	(Direct) Disclosure of subscriber information
Art. 8	Giving effect to orders 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