

# Budapest Convention on Cybercrime:

Content, impact, benefits and process of accession

Jan Kralik, Cybercrime Division  
jan.kralik@coe.int  
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

# The problem of cybercrime ...

## Cybercrime To Cost The World \$10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

f t in G+ p @ Email Print Friendly Share

November 18, 2020 11:03 ET | Source: INTRUSION Inc.

PLANO, Texas, Nov. 18, 2020 (GLOBE NEWSWIRE) -- Cybersecurity Ventures predicts global cybercrime costs will grow by 15 percent per year over the next five years, reaching \$10.5 trillion USD annually by 2025, up from \$3 trillion USD in 2015. This prediction is part of a

SECURITY

## IBM finds phishing threat to covid-19 vaccine 'cold chain'

Profile INTRUSION In Subscribe

Home » Security Bloggers Network » 40% Increase in Ransomware Attacks in Q3 2020

40% Increase in Ransomware Attacks in Q3 2020 by saptarshi das on November 16, 2020

## The Week in Ransomware - November 27th 2020 - Attacks continue

By Lawrence Abrams

## Comment les acteurs du cybercrime se professionnalisent

Par Sophy Caulier

Publié le 15 novembre 2020 à 18h00 - Mis à jour le 16 novembre 2020 à 11h59

Reservé à nos abonnés Partage f

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

News, World

## Covid-19 lockdowns drive spike in online child abuse

Post Covid, corporates see huge increase in cyber crimes

Published December 3, 2020, 6:39 AM by Agence France-Presse

ist Updated: Dec 02, 2020, 05:00 PM IST

## Artificial intelligence could be used to hack 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

## Warning: Domestic cyber terrorism on the rise in 2021

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

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

CYBER BULLYING

## 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 cyber violence. The DNA analysis will look into the different aspects of cyber violence against women related to nearly 400 million women around the world.

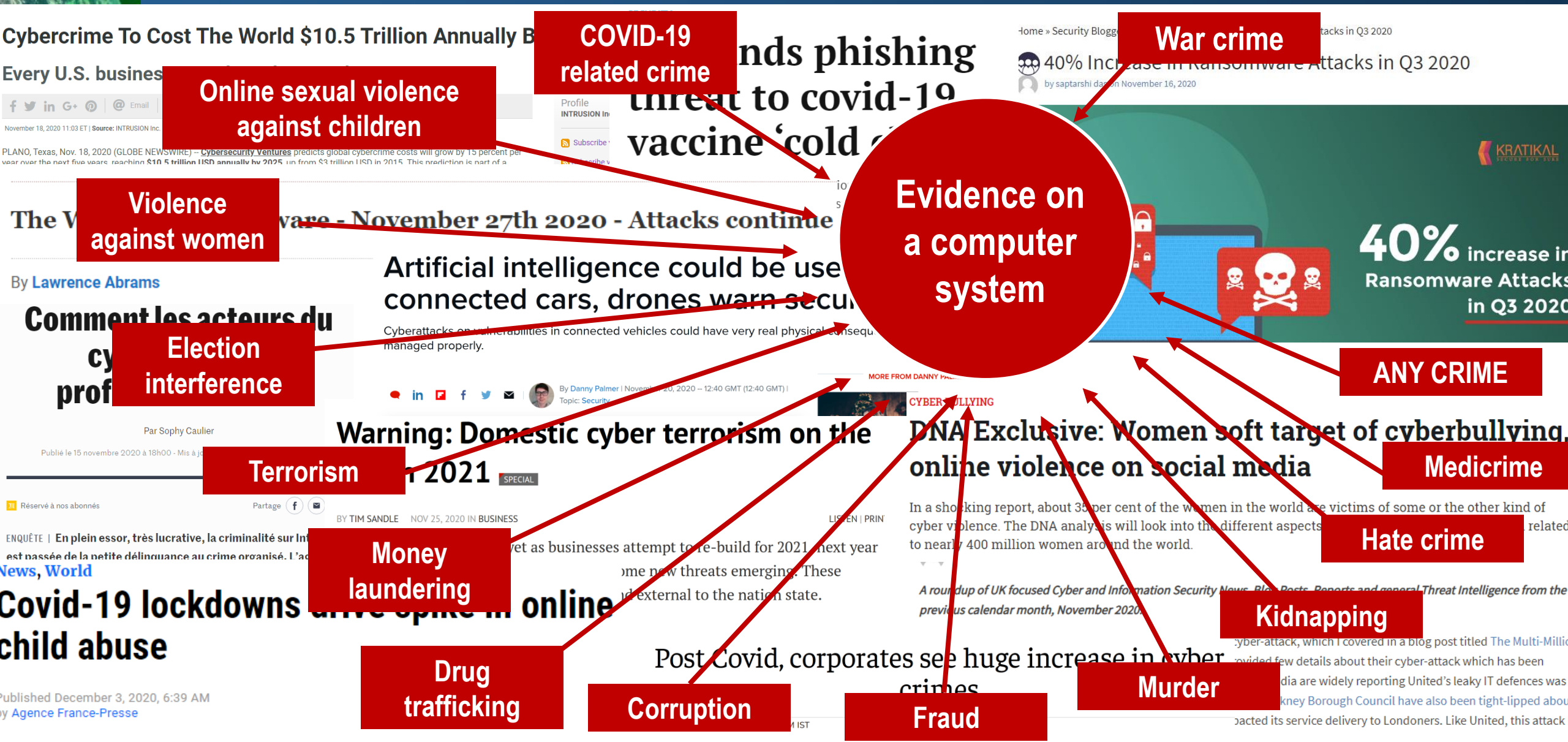
BBC NEWS Sign in Home News Sport Reel Worklife Travel

previous calendar month

Manchester United FC re Pound Manchester Unite impacting club's IT system unable to prevent a ransom what they describe as "a

## Pfizer/BioNTech vaccine docs hacked from European Medicines Agency

... and e-evidence re all types of crime



# The mechanism of the Budapest Convention

## Budapest Convention on Cybercrime (2001):

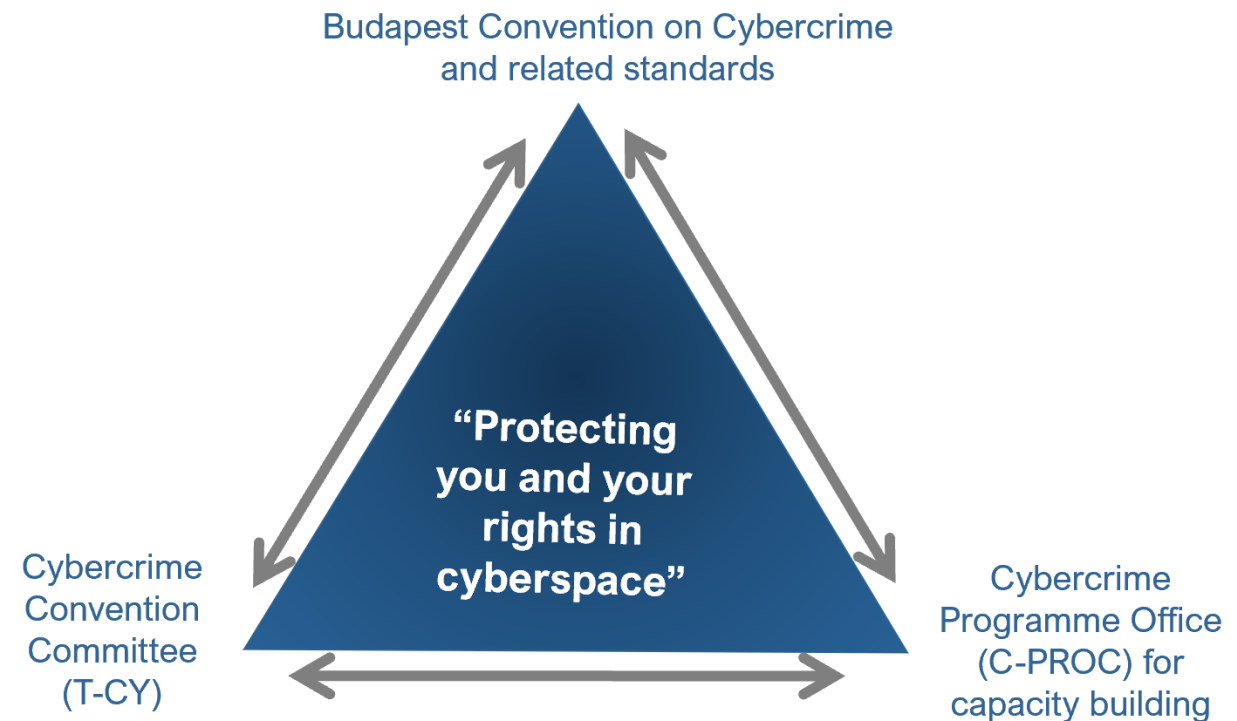
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1<sup>st</sup> Protocol on Xenophobia and Racism via Computer Systems

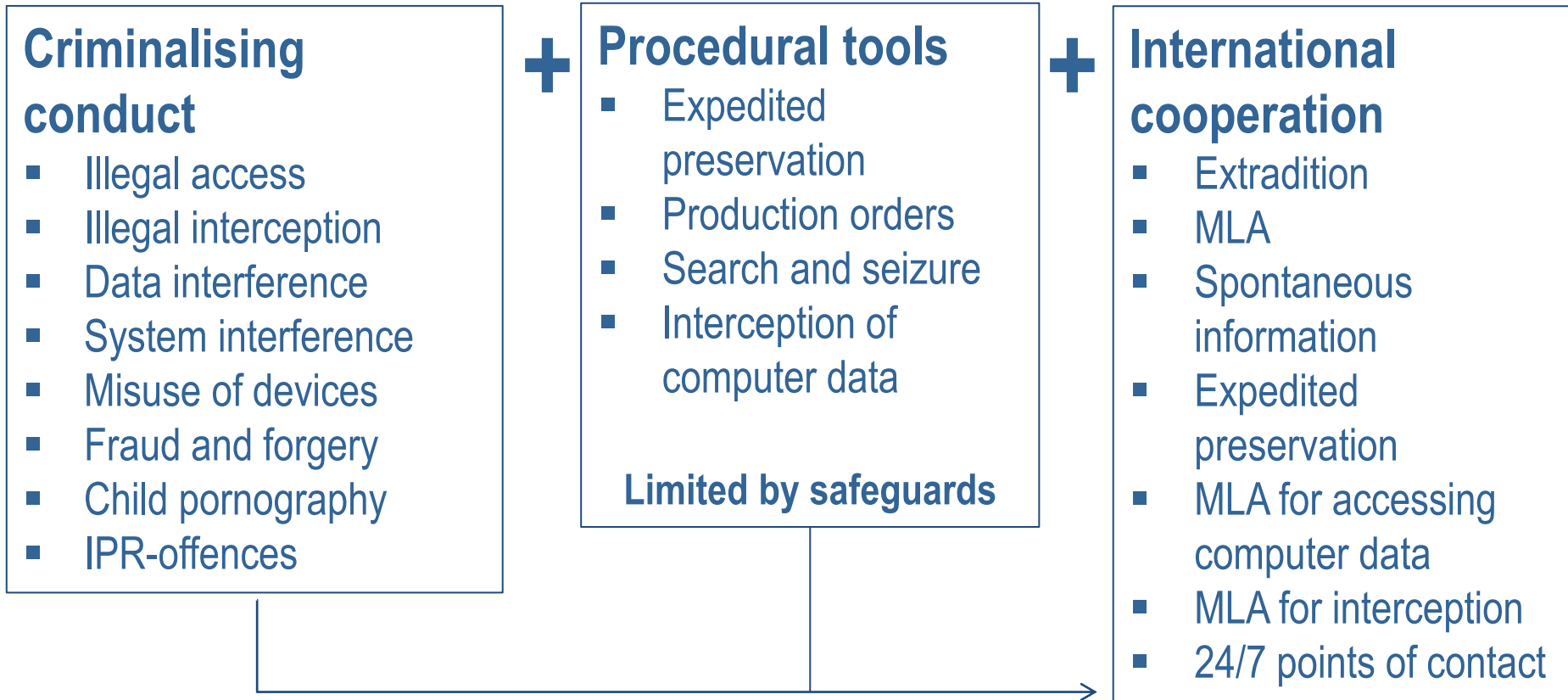
+ 2<sup>nd</sup> Protocol on enhanced cooperation on cybercrime and electronic evidence (Strasbourg, 12 May 2022)

+ Guidance Notes

**By 30 June 2023: 68 Parties and 21 Observer States**



# Content of the Budapest Convention



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

tuture tense

## How the Worst Cyberattack in History Hit American Hospitals

NotPetya caused \$10 billion in damage. But it may have also taken a toll on patients' health across the U.S.

BY ANDY GREENBERG

NOV 05, 2019 • 5:40 AM

## UK suffers third highest number of ransomware attacks globally

Based on an analysis of around 5,000 ransomware incidents, NordLocker has found that UK businesses, and small businesses in particular, are a priority target for ransomware gangs



By Sebastian Klavig Skelton, Senior reporter

Published: 28 Sep 2022 13:45

## US issues rare security alert as Montenegro battles ongoing ransomware attack

Carly Page @carlypage\_ / 3:42 PM GMT+2 • August 31, 2022

Comment



Posted 1:06PM on Thursday 12th May 2022 ( 4 months ago )

## Costa Rica declares emergency in ongoing cyber attack

f SHARE TWEET

By The Associated Press

Contact Editor

SAN JOSE, Costa Rica (AP) — After a month of crippling ransomware attacks, Costa Rica has declared a state of emergency. In theory, the measure usually reserved to deal with natural disasters or the COVID-19 pandemic would free

## The Costa Rica Ransomware Attacks: The Implications of Cyberattacks on Critical Infrastructure

Posted on August 11, 2022 by JP Perez-Etchegoyen in Best Practices

## Costa Rica's 'War' Against Ransomware Is a Wake-Up Call for the Region

James Bosworth

Jul 18, 2022



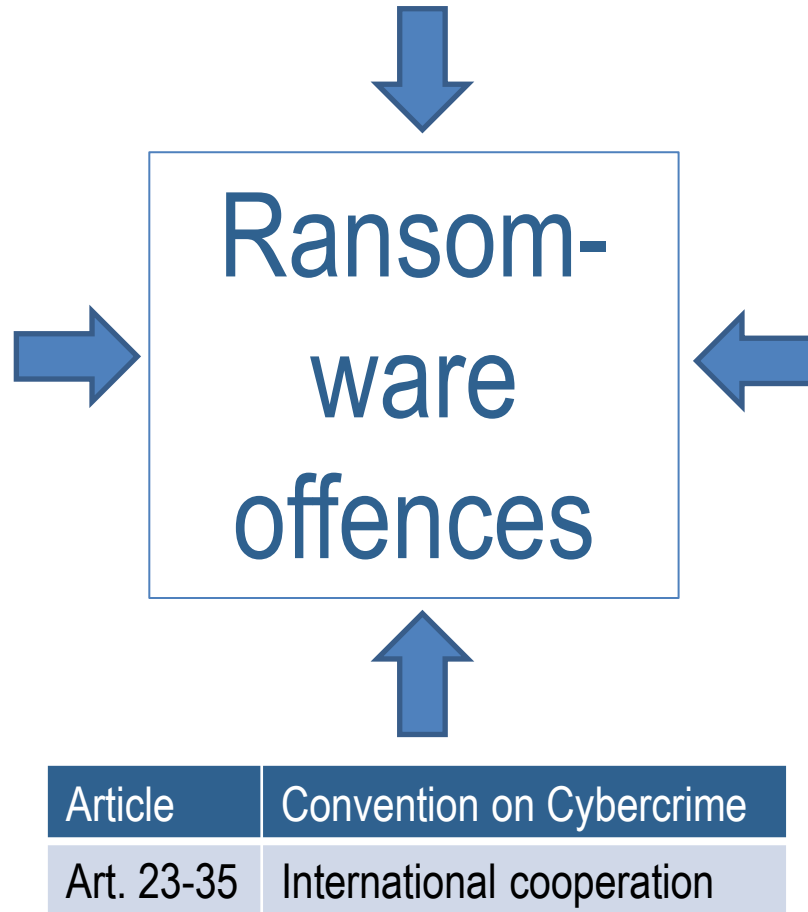
# WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017

Most first encountered ransomware after an outbreak shut down hospital computers and diverted ambulances this year. Is it here to stay?

# Content of the Budapest Convention: example ransomware

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

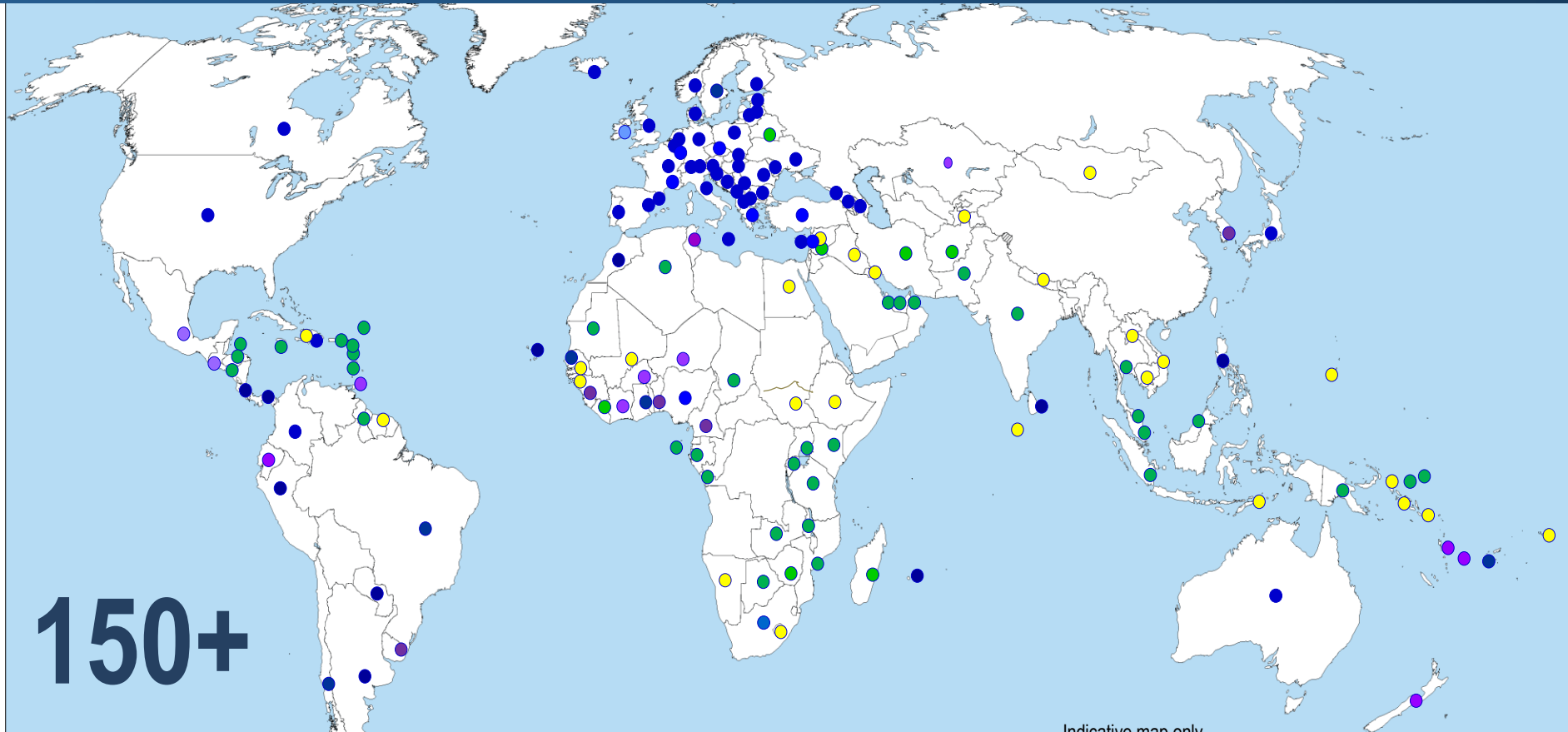
Article	Convention on Cybercrime
Art. 14-21	Procedural powers



Article	2 <sup>nd</sup> 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

Article	Convention on Cybercrime
Art. 23-35	International cooperation

# Reach of the Convention on Cybercrime



150+

Parties:	68	<span style="color: blue;">■</span>		
Signed:	2	<span style="color: blue;">■</span>	Other States with substantive laws broadly in line with Budapest Convention:	45+ <span style="color: green;">■</span>
Invited to accede:	19	<span style="color: purple;">■</span>	Further States drawing on Budapest Convention for legislation:	30+ <span style="color: yellow;">■</span>
	= 89			= 75+



## Treaty open for accession (article 37)

### Phase 1:

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

### Phase 2:

- 5 years for the completion of the process
- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

# 1<sup>st</sup> Additional Protocol to the Budapest Convention

## **Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems**

Formal adoption 7 November 2002

Opening for signature 28 January 2003

Entry into force 01 March 2006

Currently 35 State Parties

### Key provisions

- Dissemination of racist and xenophobic material through computer systems (Article 3)
- Racist and xenophobic-motivated threat (Article 4) and insults (Article 5)
- Denial, gross minimisation, approval or justification of genocide or crimes against humanity (Article 6)
- Relation between the Convention and this Protocol (Article 8)

# The first Protocol on Xenophobia and Racism: implementation

Parties		Signatories
Albania	Morocco	Canada
Andorra	Montenegro	Austria
Armenia	Netherlands	Belgium
Bosnia and Herzegovina	North Macedonia	Estonia
Croatia	Norway	Iceland
Cyprus	Paraguay	Italy
Czech Republic	Poland	Liechtenstein
Denmark	Portugal	Malta
Finland	Romania	Switzerland
France	San Marino	South Africa
Germany	Senegal	Türkiye
Greece	Serbia	
Iceland	Slovakia	
Latvia	Slovenia	
Lithuania	Spain	
Luxembourg	Sweden	
Moldova	Ukraine	
Monaco		

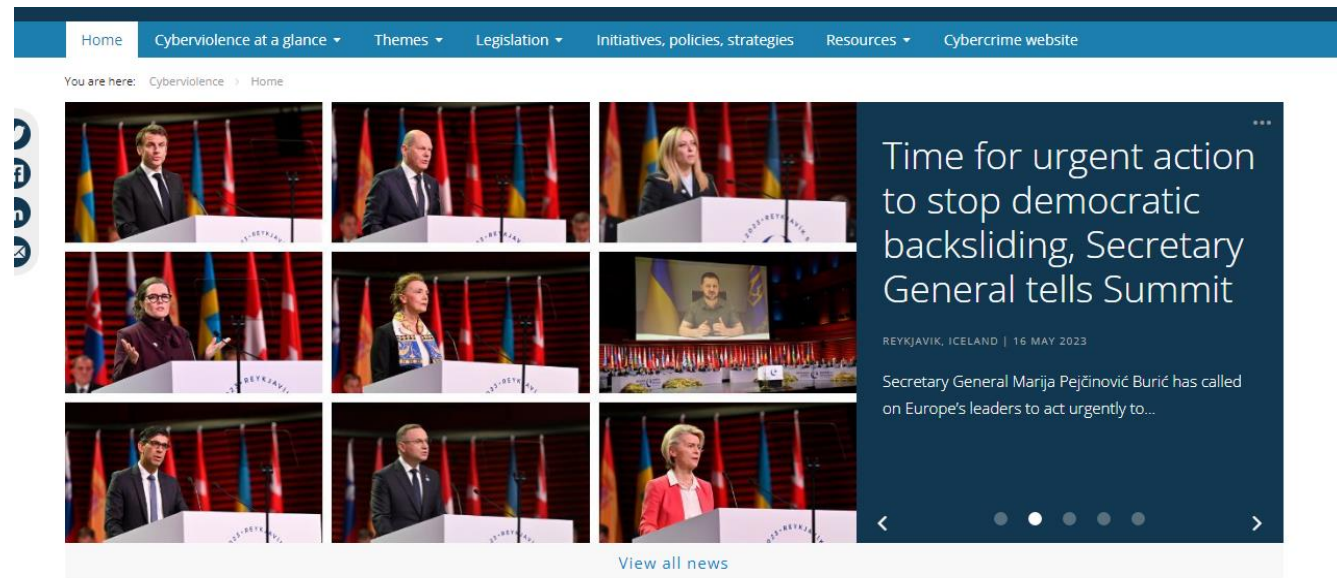
**Status as at 30 June 2023**

▶ **35 Parties + 11 Signatories**

# The first Protocol on Xenophobia and Racism: resources

## [First additional protocol dedicated page](#) :

- The official text of the protocol in official and non-official languages
- Conference
- Webinars
- [Cyberviolence webpage](#)



The screenshot shows the top navigation bar of the Cyberviolence webpage with links for Home, Cyberviolence at a glance, Themes, Legislation, Initiatives, policies, strategies, Resources, and Cybercrime website. Below the navigation bar, there is a grid of nine small images showing various individuals speaking at a podium during a summit. To the right of the grid is a large news article snippet with the headline "Time for urgent action to stop democratic backsliding, Secretary General tells Summit" and the sub-headline "Secretary General Marija Pejčinović Burić has called on Europe's leaders to act urgently to...". The article is dated "REYKJAVIK, ICELAND | 16 MAY 2023". Below the grid and article snippet is a "View all news" link.

### What is cyberviolence?

Cyberviolence being a relatively new phenomenon that **encompasses a wide variety of crimes**, the term is still difficult to define precisely. The T-CY Working Group on cyberbullying and other forms of violence, in its Mapping Study on Cyberviolence, settled on defining cyberviolence as:

### Why is addressing it important?

Cyberviolence is often misunderstood and not taken as seriously as it should be. Yet, it is important to remember that cyberviolence may start online, but it often ends offline with devastating consequences for the victims and their families. Threats of violence, stalking, incitement to suicide, solicitation of children for sexual purposes... may all result in the victim self-harming or being physically attacked by the initial perpetrator.

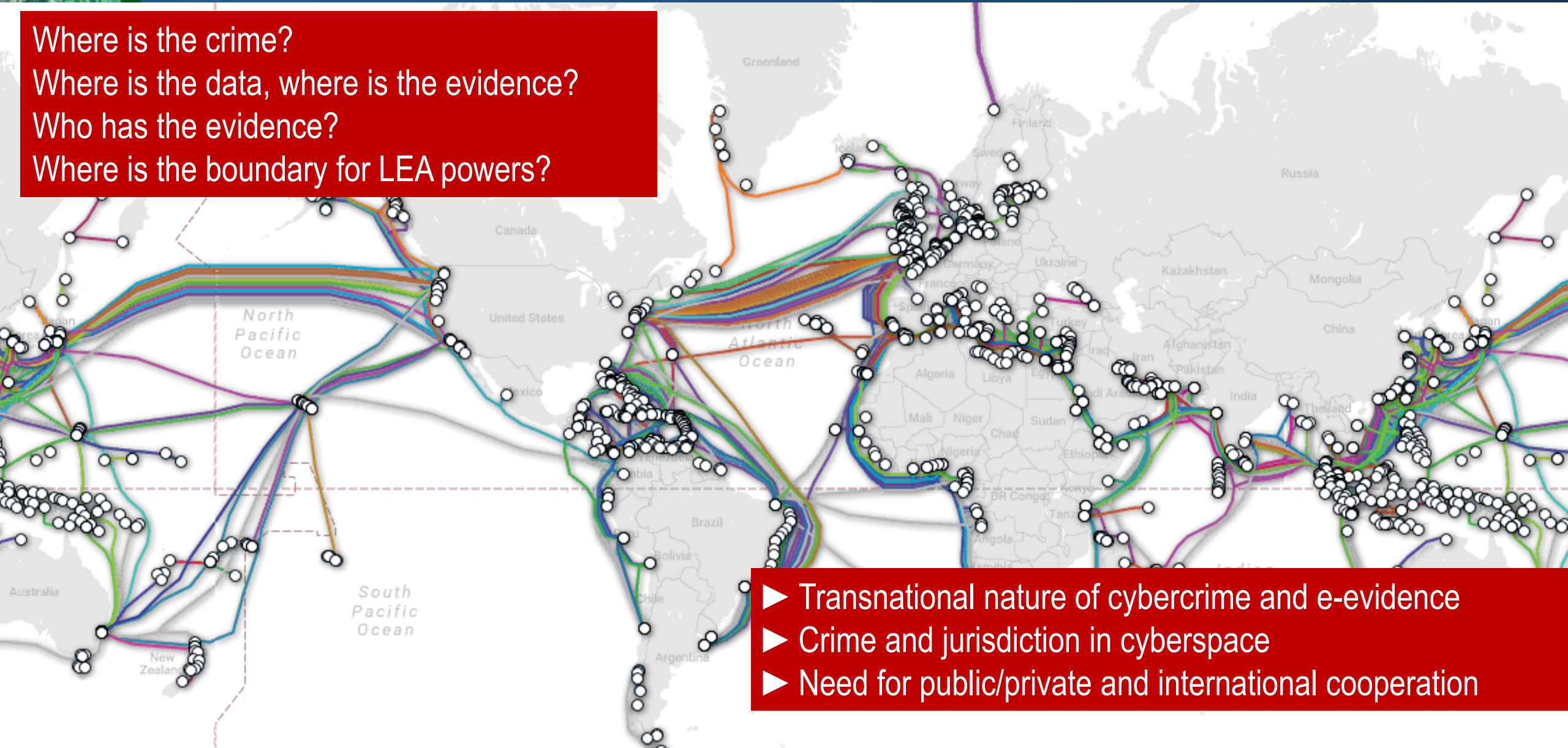
# Cybercrime and e-evidence: the problem of territoriality and jurisdiction

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

## Cybercrime: Threat to

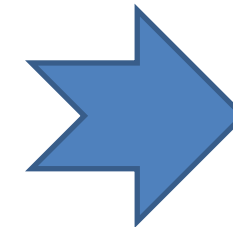
- ▶ Human rights
- ▶ Democracy
- ▶ Rule of law

## Positive obligations:

- ▶ Provide the means to protect the rights of individuals, also against crime

## Problem:

- Proliferation of cybercrime
- Any type of crime now involving e-evidence
- Evidence somewhere in foreign, multiple, shifting or unknown jurisdictions
- Effective means not available to obtain the disclosure of e-evidence
- ▶ Less than [0.1%] of offences in cyberspace lead to prosecutions and convictions
- ▶ Do victims obtain justice?



2<sup>nd</sup> Protocol to help address these challenges



# Rationale: Why a 2<sup>nd</sup> Additional Protocol to the Budapest Convention?

- ▶ How to obtain subscriber information efficiently?
- ▶ How to cooperate directly with a service provider in another Party?
- ▶ How to obtain WHOIS data (domain name registration information) from registrars?
- ▶ How to obtain stored data, including content, in an emergency situation?
- ▶ How to make mutual assistance more effective?
- ▶ How to reconcile efficient and effective measures with rule of law and data protection requirements?

# 2<sup>nd</sup> 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



# 2<sup>nd</sup> Additional Protocol to the Budapest Convention

## Protocol on enhanced cooperation and disclosure of electronic evidence

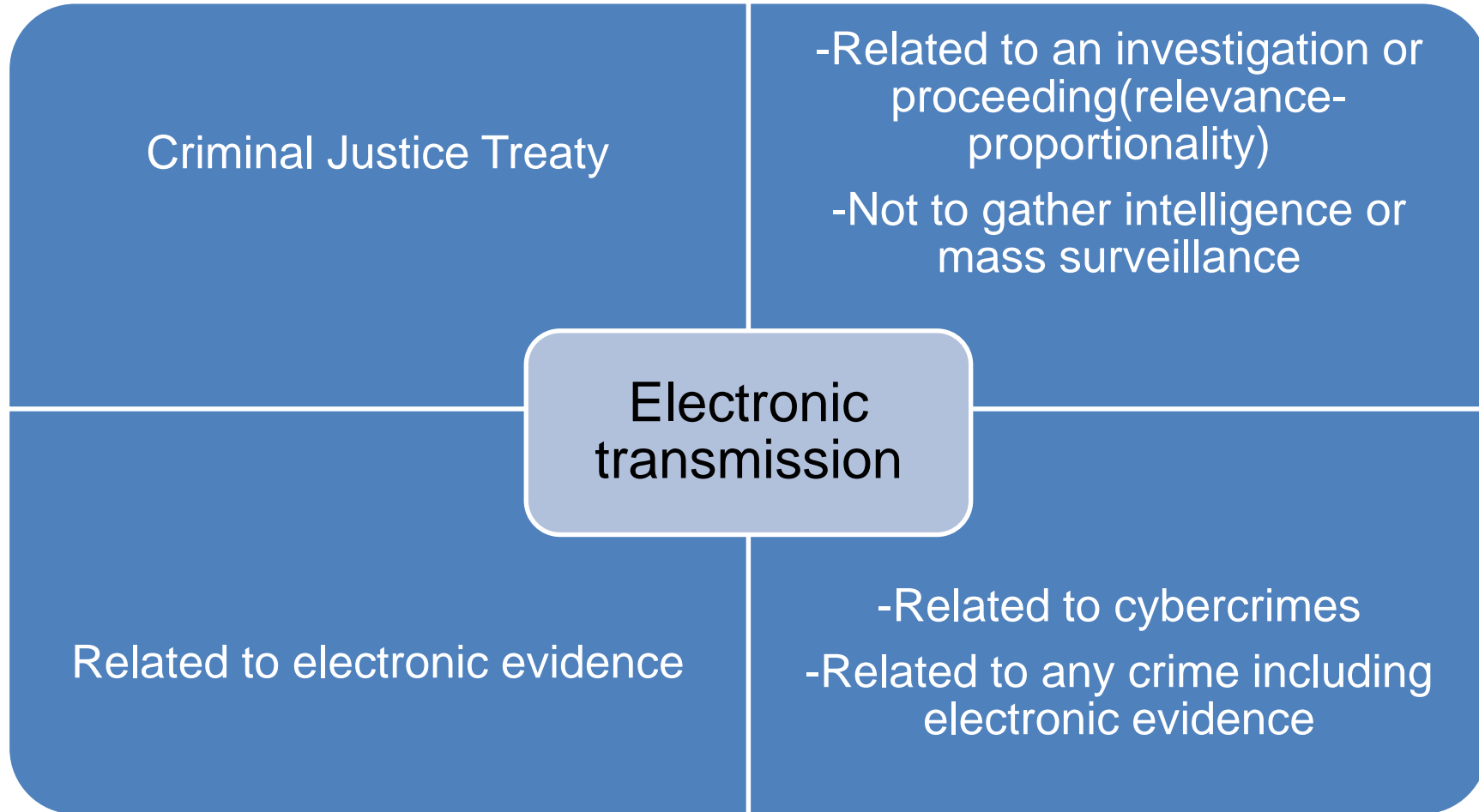
Negotiated 2017 – 2021 by Parties to the Budapest Convention

Formal adoption 17 November 2021

Opening for signature 12 May 2022

### Key provisions:

- Direct requests to registrars for data to identify registrants of domains (Article 6) or and orders to service providers to obtain subscriber information (Article 7)
- Giving effect to production orders from another Party (Article 8)
- Expedited cooperation in emergencies (Art. 9 and 10)
- Tools for mutual assistance (Article 11 - video conferencing and Article 12 – joint investigation teams and joint investigations)
- Rule of law and data protection safeguards (Articles 13 and 14)



Criminal Justice Treaty

- Related to an investigation or proceeding(relevance-proportionality)
- Not to gather intelligence or mass surveillance

Electronic transmission

Related to electronic evidence

- Related to cybercrimes
- Related to any crime including electronic evidence

# Scope – electronic transmission



## Efficiency with safeguards

### 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 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

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

Signatories (status 30 June 2023):

- |                    |                     |                    |
|--------------------|---------------------|--------------------|
| 1. Andorra         | 18. Ghana           | 35. Slovenia       |
| 2. Albania         | 19. Greece          | 36. Spain          |
| 3. Argentina       | 20. Hungary         | 37. Sri Lanka      |
| 4. Austria         | 21. Iceland         | 38. Sweden         |
| 5. Belgium         | 22. Italy           | 39. Ukraine        |
| 6. Bulgaria        | 23. Japan           | 40. United Kingdom |
| 7. Cabo Verde      | 24. Lithuania       | 41. USA            |
| 8. Canada          | 25. Luxembourg      |                    |
| 9. Chile           | 26. Malta           |                    |
| 10. Colombia       | 27. Mauritius       |                    |
| 11. Costa Rica     | 28. Montenegro      |                    |
| 12. Croatia        | 29. Moldova         |                    |
| 13. Dominican rep. | 30. Morocco         |                    |
| 14. Estonia        | 31. Netherlands     |                    |
| 15. Finland        | 32. North Macedonia |                    |
| 16. France         | 33. Portugal        |                    |
| 17. Germany        | 34. Romania         |                    |

Ratification: (status 30 June 2023): 1. Serbia

### Next:

- ▶ Signature by other Parties
- ▶ Ratification (5 needed for entry into force)
- ▶ Capacity building

## Benefits of the Protocol

### Operational value:

- Basis for direct cooperation with service providers for subscriber information (“direct disclosure”)
- Effective means to obtain subscriber information and traffic data (“giving effect”)
- Cooperation in emergencies (“expedited disclosure” + “emergency MLA”)
- Mutual assistance tools (“video-conferencing”, “JITs”)
- Data protection safeguards to permit the flow of personal data under the Protocol

### Policy value:

- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

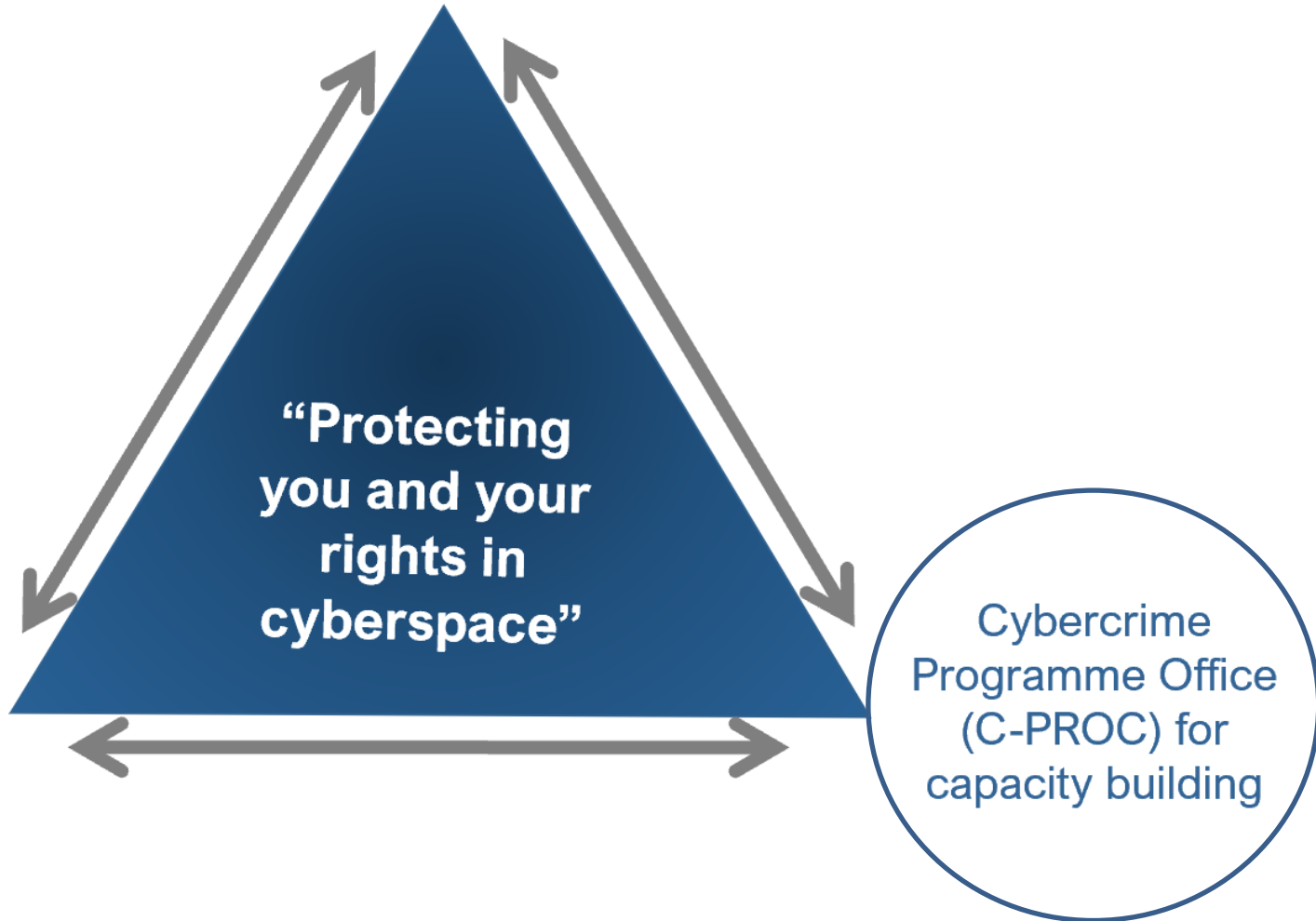
# The Convention on Cybercrime: Backed up by capacity building

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



# The Convention on Cybercrime: Backed up by capacity building



## CyberSouth: Study visit to Multinational Service Providers

6-7 JUNE 2023 | DUBLIN, IRELAND

The CyberSouth project, a joint endeavour of the Council of Europe and European Union, organised a study visit to Multinational Service Providers, to enhance public-private partnership to address cybercrime, during 6 and 7 June 2023, in Dublin, Ireland. Binance,

Google, META, Microsoft, and...



## CyberEast: Trainings on the handling of cyber incident and cybercrime taxonomy take place in the Eastern Partnership countries

29 MAY - 9 JUNE 2023 | EASTERN PARTNERSHIP REGION

Thanks to the vital contributions of project partners from Armenia, Azerbaijan, Georgia, the Republic of Moldova and Ukraine, the CyberEast joint project of the European Union and of the Council of Europe has completed a series of Training



## Octopus and GLACY+ Projects: Training on Child Protection System for countering online child sexual exploitation and abuse in Mauritius

15-19 MAY 2023 | MAURITIUS

The increasing use by children of information and communication technologies (ICTs) has created new opportunities for sexual offenders to target and harm children. As a continuation of the support to the authorities of Mauritius in fighting online child sexual exploitation and abuse (OCSEA)...



## CyberSouth: Training course on electronic evidence for judges and prosecutors

29-31 MAY 2023 | TUNIS, TUNISIA

The CyberSouth and AP-JUST projects, joint endeavours of the Council of Europe and European Union, co-organised the training course on electronic evidence for Tunisian judges and prosecutors, in co-



## GLACY+: First part of the ToT on Cybercrime and Electronic Evidence for judges and prosecutors in Peru

22-26 MAY 2023 | LIMA, PERU

Between 22-26 May 2023, was organised in Lima the first Introductory training on Cybercrime and Electronic Evidence for judges and prosecutors, since Peru's onboarding as GLACY+ priority country in 2022. The activity is part of the broader Training of Trainers (ToT) programme aimed at creating a...



## GLACY+: Co-operation with Timor-Leste on the legislative reform on cybercrime and electronic evidence

17 MAY 2023 | DILI, TIMOR-LESTE

On 17 May 2023, the GLACY+ Project, a joint action of the European Union and the Council of Europe, in co-operation with the Ministry of Justice of Timor-Leste, organised a one-day workshop to discuss the draft law currently being prepared by the national authorities in view of implementing the...



## CyberEast: Introductory and Advanced training course on cybercrime and electronic evidence for 20 Ukrainian judges

2-6 MAY 2023 | BUCHAREST, ROMANIA

Between 2-6 May 2023, the National School of Judges of Ukraine, with the support of CyberEast, a joint project of the Council of Europe and of the European Union, held an introductory training course, followed by an advanced session on cybercrime and electronic evidence, designed for judges...



## CyberEast: 25 Ukrainian investigators and prosecutors attend a training course on cybercrime and e-evidence in Suceava

25-28 APRIL 2023 | SUCEAVA, ROMANIA

CyberEast, a joint project of the European Union and of the Council of Europe, in co-operation with Police, Security services and the Prosecutor's Office training institution of Ukraine, organised a four-day exercise on cybercrime and electronic evidence in Suceava, Romania. This course was...



# The Convention on Cybercrime: Backed up by capacity building

CyberSouth: Workshop on cybercrime legislation in Jordan



Workshop on



detectives of  
(male) increas



This is the re



Union, held a

cybercrime and electronic evidence with the provisions of the Budapest Convention on...

## 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 = 1500+ since 2014
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2022
- Joint projects with the European Union
- Voluntary contributions by Canada, Hungary, Iceland, Italy, Japan, Netherlands, UK and USA in 2020-23
- Support to T-CY

ing national delivery of an introductory course  
d electronic evidence in Benin

U, BENIN

ember, a group of judges and prosecutors from Benin, who had  
ted workshop earlier in August, delivered for the first time an  
ce to their peers. During the first...

onom  
opera

### Current projects:

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

ACY+: 9th Africa Working Group on  
in Rwanda

IDA

3 partner of the GLACY+ Project, organised the 9th Africa Working  
in Rwanda from 18 to 22 July 2022. The AF-WGM is an annual  
t practices in the region. This...

# The Convention on Cybercrime: Backed up by capacity building

## CyberSouth: Workshop on cybercrime legislation in Jordan

21-22 SEPTEMBER 2022 | JORDAN

### Projects managed by C-PROC support:

- ▶ Strengthening legislation on cybercrime and electronic evidence in line with rule of law and human rights (including data protection) standards
- ▶ Training judges, prosecutors and law enforcement officers
- ▶ Establishing specialized cybercrime and forensic units and improving interagency cooperation
- ▶ Promoting public/private cooperation
- ▶ Protecting children against sexual violence online
- ▶ Enhancing the effectiveness of international cooperation

## GLACY+: Supporting national delivery of an introductory course on cybercrime and electronic evidence in Benin

2 SEPTEMBER 2022 | COTONOU, BENIN

### Rationale:

Support countries in the implementation of the Convention on Cybercrime

- ▶ Priority given to countries that are Parties to or that have requested accession to the Convention on Cybercrime

## INTERPOL and GLACY+: 9th Africa Working Group on Cybercrime meets in Rwanda

18-22 JULY 2022 | KIGALI, RWANDA

INTERPOL, as implementing partner of the GLACY+ Project, organised the 9th Africa Working Group Meeting on Cybercrime for Head of Units (AF-WGM) in Rwanda from 18 to 22 July 2022. The AF-WGM is an annual event that aims to facilitate sharing of information and best practices in the region. This...

## Workshop on domestic legislation

PANAMA&ONLINE | 15 SEPTEMBER 2022

On 15 September, the Council of Europe, through the GLACY+ joint project with the European Union, held a hybrid workshop with the authorities of Panama in view of further harmonising national legislation on cybercrime and electronic evidence with the provisions of the Budapest Convention on...

## Benefits

- ✓ Stronger and more consistent legislation
- ✓ More efficient international cooperation between Parties
- ✓ More investigation, prosecution, adjudication of cybercrime and e-evidence cases
- ✓ Trusted partnerships and public/private cooperation
- ✓ Catalyst for capacity building
- ✓ Better cybersecurity performance
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Contribution to human rights/rule of law in cyberspace

“Cost”: Commitment to cooperate

**Disadvantages?**

The background features a dark, abstract composition of green and blue digital patterns, resembling data streams or network connections. A prominent blue banner with a white underline is centered horizontally across the image.

[www.coe.int/cybercrime](http://www.coe.int/cybercrime)