



# THE UNDERGROUND ECONOMY 2022

5-8 September 2022, Strasbourg, France

Enhanced co-operation and disclosure of electronic evidence:

The Second Additional Protocol to the Convention on Cybercrime

Alexander Seger  
Executive Secretary  
Cybercrime Convention Committee  
Council of Europe



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

1



## The problem of cybercrime ...

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

Every U.S. business is under cyberattack

November 18, 2020 11:03 ET | Source: NETWORKS

PLANO, Texas, Nov. 18, 2020 (SLOBE NEWSWIRE) - **Cybersecurity Ventures** predicts global cybercrime costs will grow by 15 percent per year from the most that value security \$18.4 billion (USD) annually for 2019, to from \$1 trillion (USD) in 2024. This translates to an all of 3

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

40% Increase in Ransomware Attacks in Q3 2020

By [Sagar Choudhary](#) on November 20, 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 19h00

### 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.

### 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 threats are external to the nation state.

News, World

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

Post Covid, corporates see huge increase in cybercrimes

Published December 3, 2020, 6:39 AM  
by [Agence France-Presse](#)

Not Updated Dec 02, 2020, 05:00 PM EST

2

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

**Evidence on a computer system**

- COVID-19 related crime
- WARCRIME
- Online sexual violence against children
- Violence against women
- Election interference
- Terrorism
- Money laundering
- Financial crime
- Corruption
- Fraud
- Murder
- Kidnapping
- Hate crime
- Medicrime
- ANY CRIME
- DNA Exclusive: Women soft target of cyberbullying, online violence on social media
- 40% Increase in Ransomware Attacks in Q3 2020

3

## The mechanism of the Convention on Cybercrime

### Budapest Convention on Cybercrime (2001):

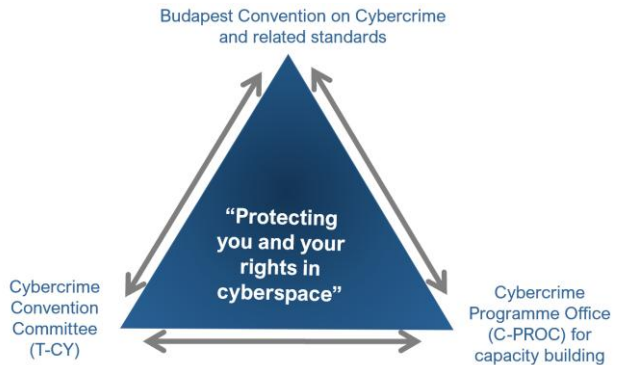
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

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

+ Guidance Notes

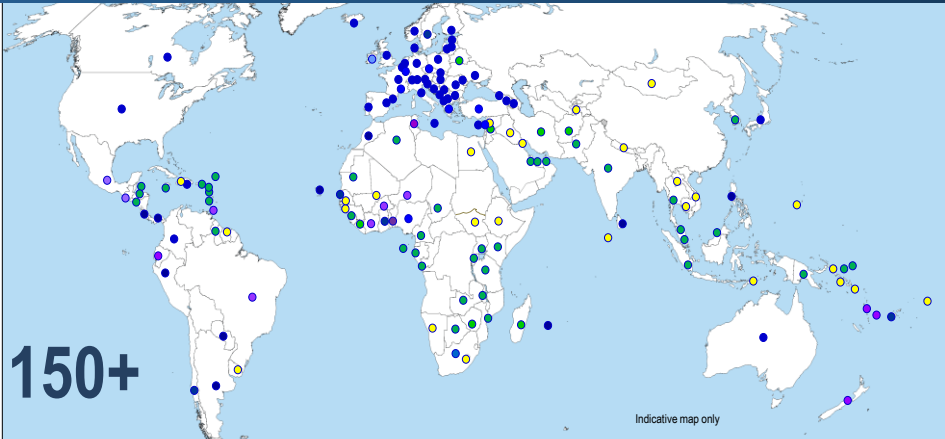
+ 2<sup>nd</sup> Protocol on enhanced cooperation on cybercrime and electronic evidence (opened for signature 12 May 2022)

By August 2022: **67 Parties and 15 Observer States**



4

Reach of the Convention on Cybercrime



Parties:	67			
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+	
	= 82		= 75+	

5

Why a new Protocol?

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

6



## 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?

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

7



## 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

8



## 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime: safeguards

### 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

9



## 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime: next

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

Signatories (status 15 August 2022):

- |               |                     |
|---------------|---------------------|
| 1. Andorra    | 13. Lithuania       |
| 2. Austria    | 14. Luxembourg      |
| 3. Belgium    | 15. Montenegro      |
| 4. Bulgaria   | 16. Morocco         |
| 5. Chile      | 17. Netherlands     |
| 6. Colombia   | 18. North Macedonia |
| 7. Costa Rica | 19. Portugal        |
| 8. Estonia    | 20. Romania         |
| 9. Finland    | 21. Serbia          |
| 10. Iceland   | 22. Spain           |
| 11. Italy     | 23. Sweden          |
| 12. Japan     | 24. USA             |

#### Next:

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

10



## 2<sup>nd</sup> Additional Protocol to the Convention on Cybercrime: benefits

### Benefits of the Protocol

#### Operational value:

- Legal basis for disclosure of WHOIS information
- 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)