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

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

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

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

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

By Lawrence Abrams

Comment les acteurs du cybercrime se professionnalisent

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.

40% Increase in Ransomware Attacks in Q3 2020

40% increase in Ransomware Attacks in Q3 2020

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 relate to nearly 400 million women around the world.

Warning: Domestic cyber terrorism on the rise in 2021

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.

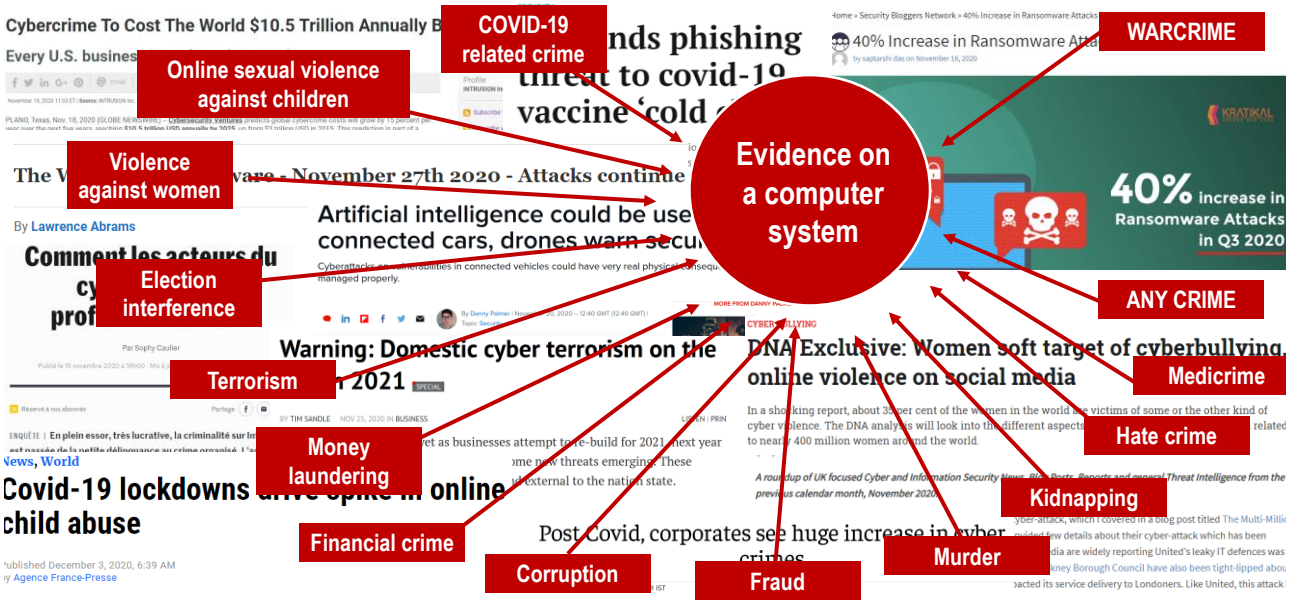
Covid-19 lockdowns drive spike in online child abuse

Post Covid, corporates see huge increase in cyber crimes

Pfizer/BioNTech vaccine docs hacked from European Medicines Agency

2

… and e-evidence re all types of crime



3

The mechanism of the Convention on Cybercrime

Budapest Convention on Cybercrime (2001):

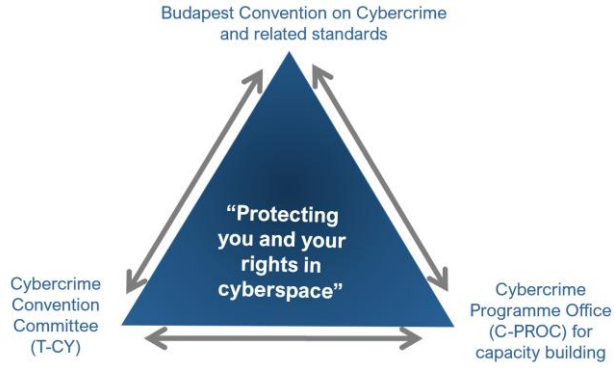
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

+ Guidance Notes

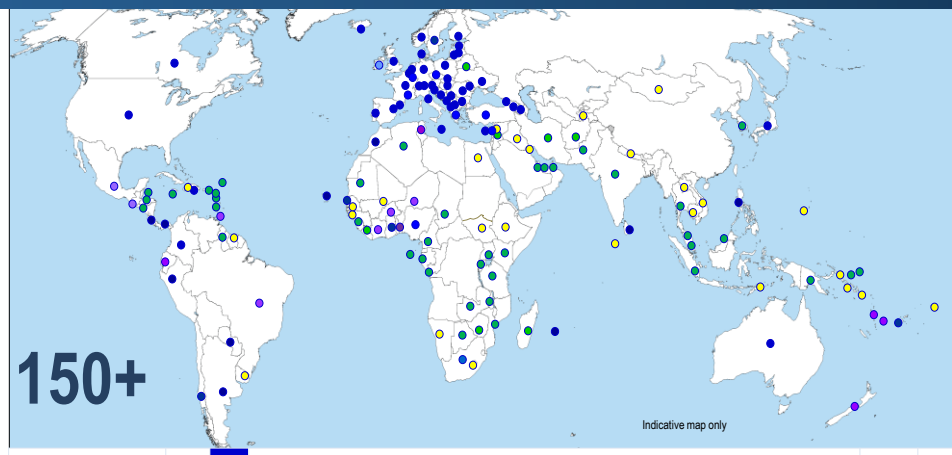
+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence (opened for signature 12 May 2022)

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?

2nd Protocol to help address these challenges

www.coe.int/cybercrime

6

Rationale: Why a 2nd 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?

2nd Additional Protocol to the Convention on Cybercrime: content

2nd 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

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 15 August 2022):

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

Next:

► Signature by other Parties

► Ratification (5 needed for entry into force)

► Capacity building

10

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)