



ROLE OF PROSECUTORS IN THE PROTECTION OF INDIVIDUAL RIGHTS AND PUBLIC INTEREST IN LIGHT OF REQUIREMENTS OF THE EUROPEAN CONVENTION ON HUMAN RIGHTS“

*High-Level International Conference co-organised by the Russian General Prosecutor's Office,
the Council of Europe and the International Association of Prosecutors*

Second Session of the Conference:
Prosecutor's Supervision over Compliance with Legislation

Cooperation on cybercrime: the approach of the Council of Europe

Pedro Verdelho
Cybercrime Committee (T-CY) of the
Council of Europe



Why is the Council of Europe dealing with 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'

ion efforts...without the right s
sn't stand a chance.

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

Réservé 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

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



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.

LISTEN | PRINT

per Sec

urityExpert on

f UK focused

previous calendar month

Manchester United FC re

Pound Manchester Unite

impacting club's IT syste

unable to prevent a ransi

what they describe as "a

NEWS

Home | Coronavirus | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Health

Tech

Pfizer/BioNTech vaccine docs hacked from European Medicines Agency

Why is the Council of Europe dealing with cybercrime

- Theft of personal data
- Online child sexual abuse
- Cyberbullying, harassment and others forms of cyberviolence
- Fraud generating crime proceeds
- Attacks against critical information infrastructure
- Ransomware
- Election interference
- COVID-19 related cybercrime



Threats to

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

What is the approach of the Council of Europe: 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

+ Guidance Notes

+ Protocol on Xenophobia and Racism via Computer Systems (2003)

+ 2nd Protocol on enhanced cooperation and disclosure of electronic evidence in preparation

By May 2021: 66 Parties and 11 Observer States

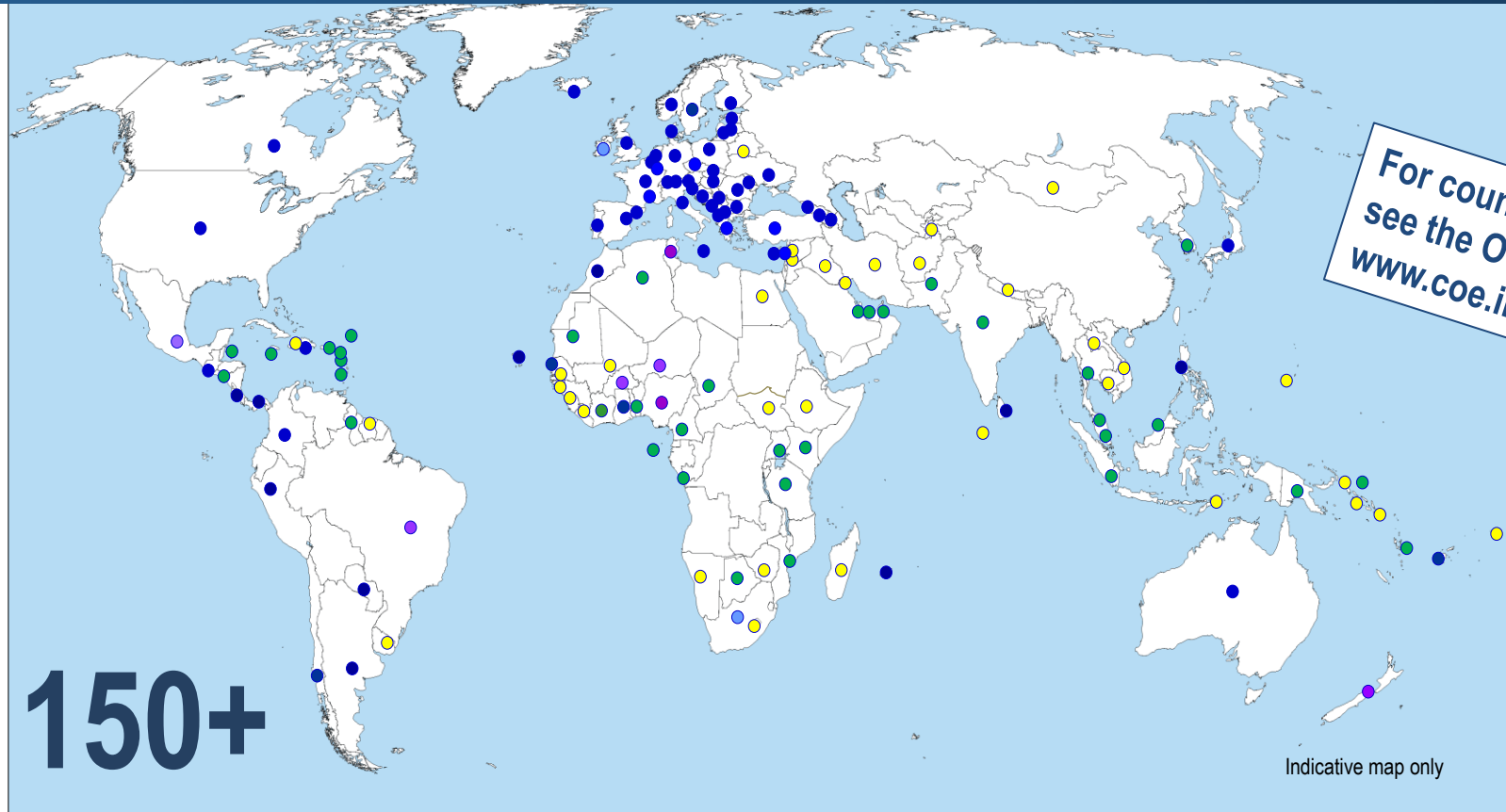
1 Common standards: Budapest Convention on Cybercrime and relates standards

**2 Follow up and assessments:
Cybercrime
Convention
Committee (T-CY)**



**3 Capacity building:
C-PROC ►
Technical cooperation
programmes**

Reach of the Budapest Convention



Parties:

66



Other States with laws largely in line with

Signed:

2



Budapest Convention = 20+



Invited to accede:

9



Further States drawing on Budapest Convention for legislation = 50+



=

77

Why a new Protocol?

- The scale and quantity of cybercrime, devices, users and victims
- Cloud computing, territoriality and jurisdiction
 - Where is the crime?
 - Where is the data, where is the evidence?
 - Who has the evidence?
 - What legal regime applies to order / disclose data?
- The challenge of mutual legal assistance
- The “<1% problem”

- ▶ 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?



Draft 2nd Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence: 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

Section 1 – General principles applicable to Chapter II

- Article [5] General principles applicable to Chapter II

Section 2 – Procedures enhancing direct cooperation with providers and entities in other Parties

- Article [6] Request for domain name registration information
- Article [7] Disclosure of subscriber information

Section [3] – Procedures enhancing international cooperation between authorities for the disclosure of stored computer data

- 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

Section [4] – Procedures pertaining to emergency mutual assistance

- Article [10] Emergency mutual assistance

Section [5] – Procedures pertaining to international cooperation in the absence of applicable international agreements

- 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

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”)
- Legal basis for disclosure of WHOIS information
- 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)

- ▶ Specific and limited measures against cybercrime v. Control of information in cyberspace
- ▶ Laws on cybercrime used to prosecute speech
- ▶ How to ensure data protection and procedural rights in a cross-border context?
- ▶ “Cyber” affects core interest of States, private sector, individuals & difficult international context
 - Difficult to reach agreement, find common ground
 - Risk of greater international polarisation
- ▶ Any international initiative on cybercrime should
 - be based on consensus to permit more cooperation and avoid further divisions / polarisation
 - meet human rights and rule of law requirements to maintain a free and open internet
 - meet the needs of criminal justice practitioners
 - be consistent with existing standards

In this context ► Budapest Convention in place and functioning

- The “mechanism” of the Budapest Convention
- Reach ► Rolling out the Convention
- Ensuring quality ► T-CY
- Building capacities to implement ► C-PROC
- Reconciling effective measures on cybercrime with human rights and rule of law requirements
- Keeping up-to-date ► Guidance Notes, Protocols