Action on cybercrime and electronic evidence:

Budapest Convention and its Second Protocol on electronic evidence

Jan Kralik
Cybercrime Division
www.coe.int/cybercrime

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

The problem of cybercrime …

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

Email | Print Friendly | Share

Profile

FBI Reports $12.5 Billion Increase in Losses from Cybercrime Amid Ongoing Phishing Attacks

APRIL 8, 2024 | TECHNOLOGY

SECURITY

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

Cyberattackers are targeting vaccination efforts... without the right s measures in place, your business doesn't stand a chance.

3 December 2020

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

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 11h5

Réservé à nos abonnés | Partage

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

Generative AI is making phishing attacks more dangerous

Warning: Domestic cyber terrorism on the rise in 2021 SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS LISTEN | PRIN

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 include new cyber-threats, both internal and 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 relate to nearly 400 million women around the world.

Alarming escalation in child sexual abuse online revealed by Global Threat Assessment 2023

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

BBC | Sign in | Home | News | Sport | Reel | Worklife | Travel

NEWS

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

Tech

Pfizer/BioNTech vaccine docs hacked from European Medicines Agency

… and e-evidence re all types of crime

Evidence on a computer system

COVID-19 related crime

War crime

Online sexual violence against children

Violence against women

Election interference

Terrorism

Money laundering

Drug trafficking

Corruption

Fraud

Murder

Kidnapping

Hate crime

Medicrime

ANY CRIME

Cybercrime To Cost The World $10.5 Trillion Annually B

Every U.S. busines

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

nds phishing

threat to covid-19

vaccine 'cold

Home » Security Blogg

tacks in Q3 2020

40% Increase in Ransomware Attacks in Q3 2020

by saptarshi da on November 16, 2020

The V vare - November 27th 2020 - Attacks continue

By Lawrence Abrams

Comment les acteurs du cy

prof

Par Sophy Caulier

Publié le 15 novembre 2020 à 18h00 - Mis à jo

Réservé à nos abonnés

Partage

Artificial intelligence could be use

connected cars, drones warn secu

Cyberattacks on vulnerabilities in connected vehicles could have very real physical consequ

managed properly.

By Danny Palmer | Novem 20, 2020 -- 12:40 GMT (12:40 GMT) |

Topic: Security

Warning: Domestic cyber terrorism on the

2021 SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

LISTEN | PRIN

vet as businesses attempt to re-build for 2021 next year

me new threats emerging. These

d external to the nation state.

MORE FROM DANNY PA

CYBERBULLYING

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 related to nearly 400 million women around the world.

ENQUÊTE | En plein essor, très lucrative, la criminalité sur Int

est passée de la petite délinquance au crime organisé. L'ac

News, World

Covid-19 lockdowns drive spike in online child abuse

Published December 3, 2020, 6:39 AM

by Agence France-Presse

A roundup of UK focused Cyber and Information Security News, Blog Posts, Reports and general Threat Intelligence from the previous calendar month, November 2020.

Post Covid, corporates see huge increase in cyber crimes

cyber-attack, which I covered in a blog post titled The Multi-Millio

provided few details about their cyber-attack which has been

dia are widely reporting United's leaky IT defences was

kney Borough Council have also been tight-lipped abou

pacted its service delivery to Londoners. Like United, this attack

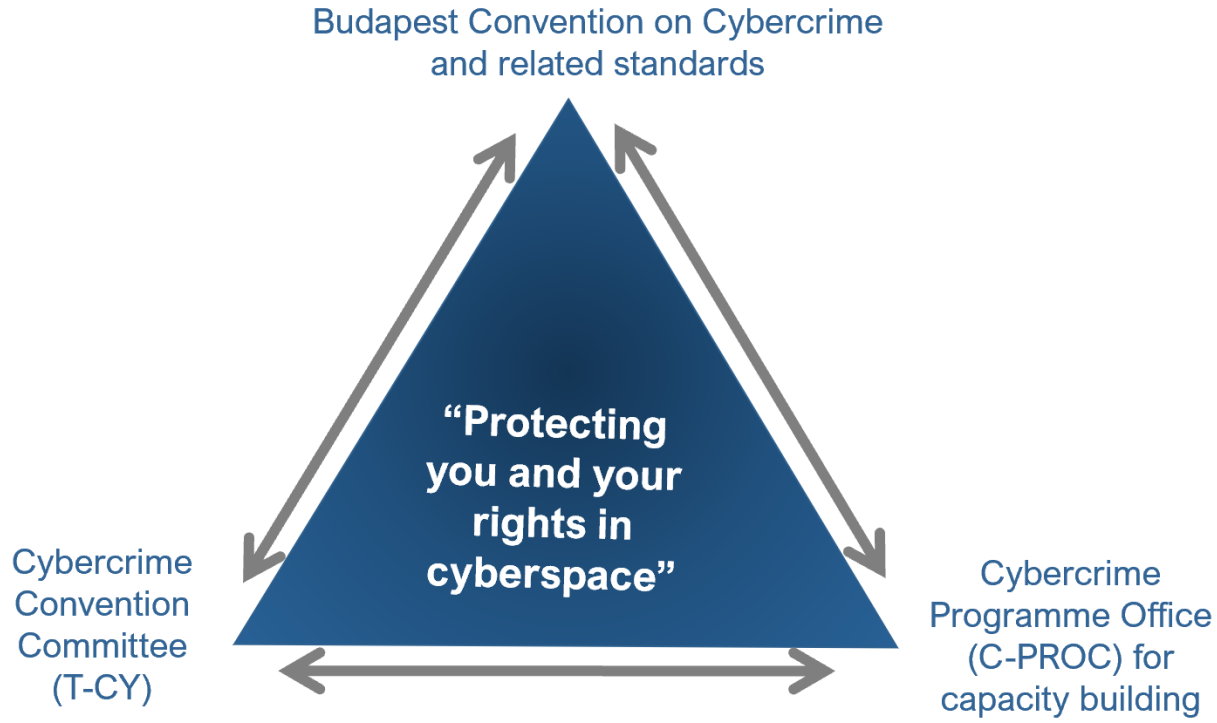
The mechanism of the Budapest Convention

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

+ 1st Protocol on Xenophobia and Racism via Computer Systems
+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence (Strasbourg, 12 May 2022)
+ Guidance Notes

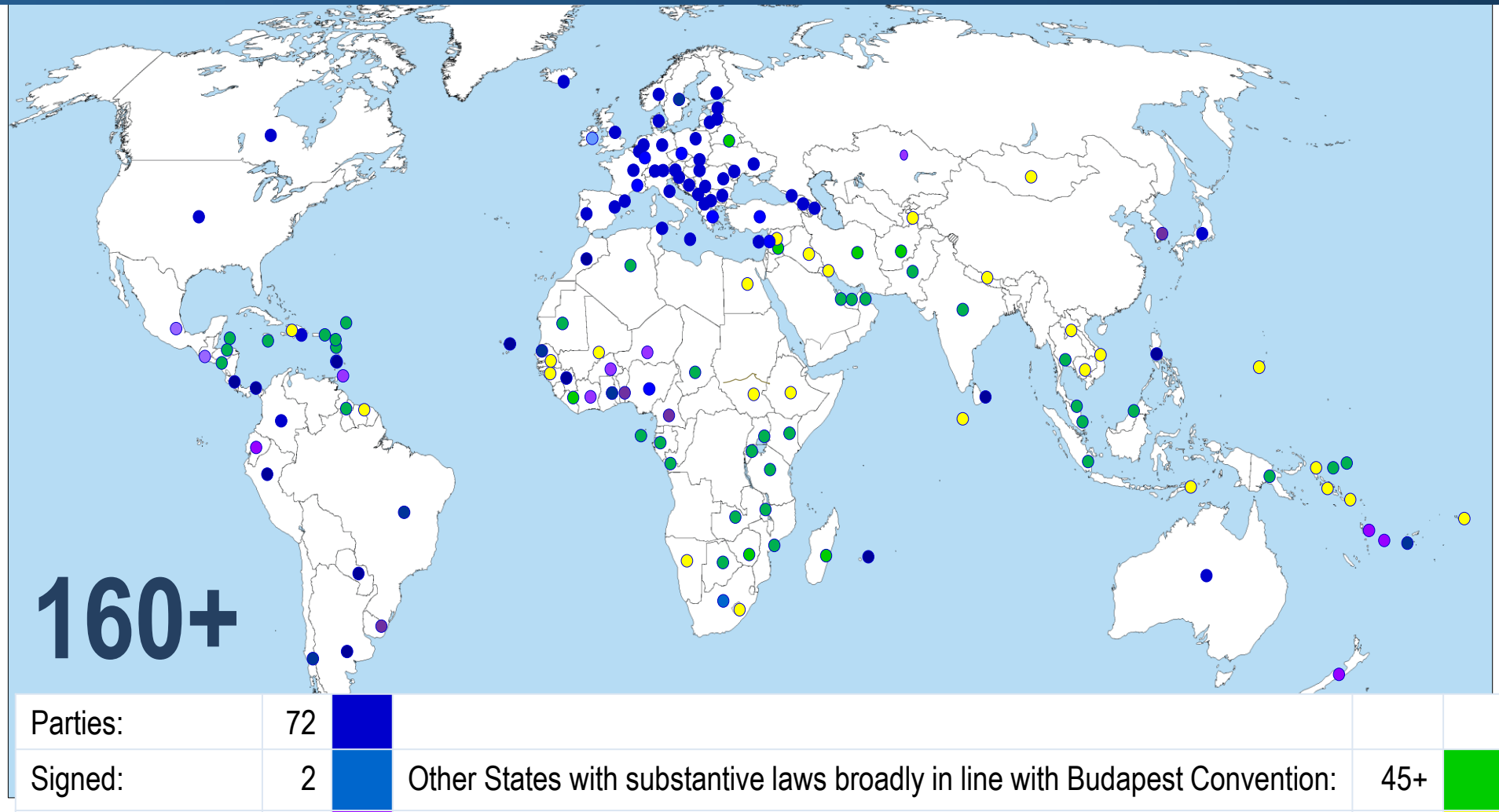
By 24 April 2024: 72 Parties and 21 Observer States



Practical guidelines that can help law enforcement and service providers organise their cooperation

- include common guidelines for both law enforcement and service providers and specific guidelines for each of them
- are not to substitute legislation or other formal regulations, but rather to supplement and help regulations work in practice
- are based on good practices already available
- are to be adapted to the specific circumstances in each country.

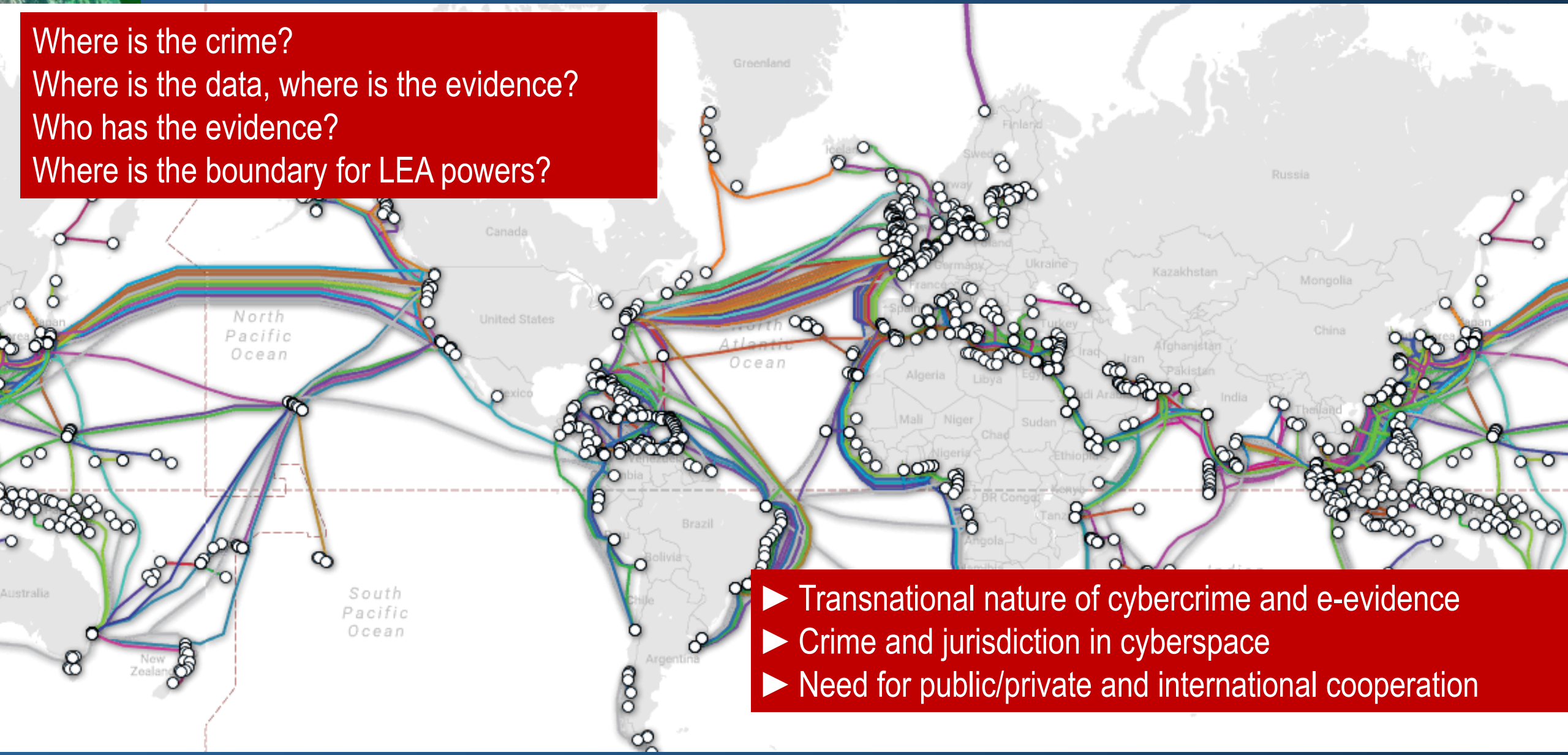
Reach of the Convention on Cybercrime



Parties:	72				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	19		Further States drawing on Budapest Convention for legislation:	30+	
=	**93**		=	**75+**	

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

Why a new Protocol?

Cybercrime: Threat to

- Human rights
- Democracy
- Rule of law

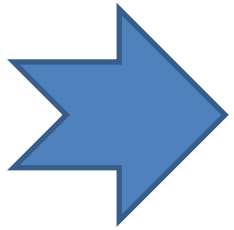
Positive obligations:

- 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

2nd 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 and orders to service providers for data to identify registrants of domains (Article 6) or subscribers of services (Article 7)
- Giving effect to production orders from another Party (Article 8)
- Expedited cooperation in emergencies (Articles 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)

2nd Additional Protocol to the Convention on Cybercrime: **effective tools + strong 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 particularly 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

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:

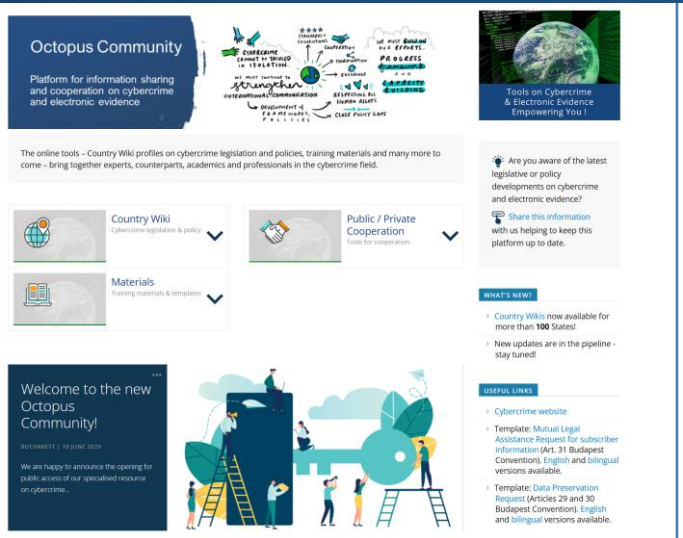
- Convention on Cybercrime will remain relevant and effective
- Efficient cooperation with rule of law and data protection safeguards is feasible
- Respect for free Internet with limited restrictions in case of criminal misuse (specific criminal investigations, specified data)

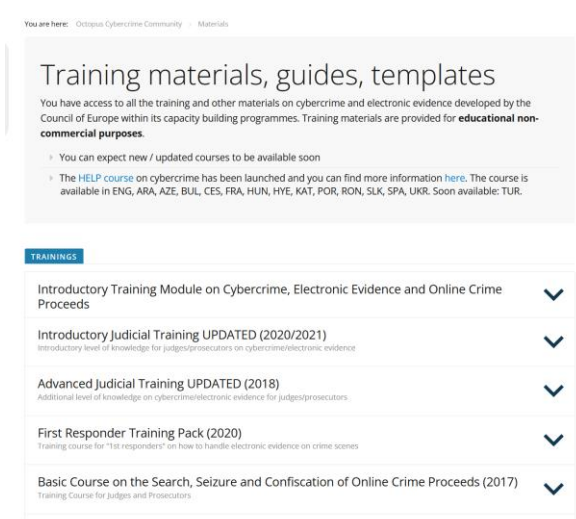
Ten years of capacity building on cybercrime: Guides, tools, resources

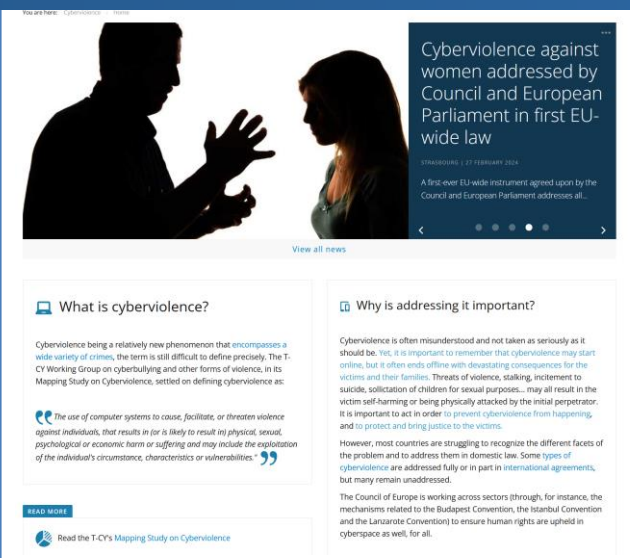
Octopus Project

Discussion paper:
Freedom of expression within the context of action on cybercrime – Practical considerations

Strasbourg, 10 December 2023 / Provisional version







Octopus Project

Implementing the First Protocol to the Convention on Cybercrime on Xenophobia and Racism: Good practice study

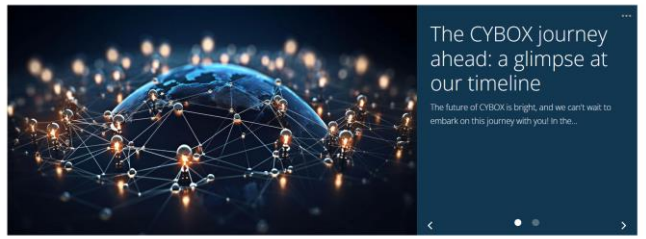
Strasbourg, 1 December 2023 (provisional)

Country Wiki

The wiki profiles provide an overview of a country's policy on cybercrime and electronic evidence. Every fiche includes a description of cybercrime policies/strategies, the state of cybercrime legislation, the channels of cooperation, international cooperation and case law.

For more information on a country's legislation, click on the legal profile in each country wiki.

CYBOX
CYBERCRIME & E-EVIDENCE
COUNCIL OF EUROPE
CONSEIL DE L'EUROPE



ABOUT CYBOX:

Welcome to **CYBOX** – your online platform for exchange, training, and resource sharing on cybercrime and electronic evidence.

With the rise of cybercrime and the increasing reliance on electronic evidence, it is essential for professionals in the criminal justice sector to stay ahead of the criminals. **CYBOX** is designed to meet the evolving training needs of judges, prosecutors, law enforcement agencies, and other key stakeholders in the criminal justice system worldwide.

CYBOX creates an environment in which countries cooperating with

A repository of cybercrime and e-evidence related reference and training materials

Highly customizable **learning management system** for C-PROC and criminal justice

C-PROC

The global state of cybercrime legislation 2013 – 2023: A cursory overview

Bucharest, 8 December 2023 / Provisional version