Session on domestic and international frameworks on cybercrime and e-evidence: their relevance for the COVID-19 pandemic

International frameworks: The tools of the Budapest Convention on Cybercrime

Alexander Seger
Head of Cybercrime Division
Council of Europe

Reminder: the problem of cybercrime …

Cybercrime

► Offences against and by means of computers

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: INTRUSION Inc.

PLANO, Texas, Nov. 18, 2020 (GLOBE NEWSWIRE) -- Cybersecurity Ventures predicts global cybercrime costs will g
year over the next five years, reaching $10.5 trillion USD annually by 2025, up from $3 trillion USD in 2015. This pre

SECURITY

Online child abuse racket: CBI raids 77 spots,

Raj Sekhar / TNN / Updated: Nov 17, 2021, 09:26 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

The Week in Ransomware - Novemb

By Lawrence Abrams

Artifi
conn

Cyberattack
managed pr

soft target of cyberbullying
l media

en in the world are victims of some or the other kind of
different aspects of cyber violence against women relate

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

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

Warning:
rise in 20

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

This year has been rocky, yet as businesses attempt to re-build for 2
will see a continuation of challenges and some new threats emergir
l external to the nation

Child protection

Fifteen times more child sexual abuse material found online than 10 years ago

Experts from Internet Watch Foundation demand UK uses online safety bill to protect children

News, World

Covid-19 lockdowns drive spike in online child abuse

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

Post Covid, corporates see huge increase in cyb
crimes

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

Sarah Marsh

@sloumarsh

Sat 13 Nov 2021 07.00 GMT

… and e-evidence re all types of 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

Online sexual violence against children

COVID-19 related crime

nds phishing

threat to covid-19

vaccine 'cold

Violence against women

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

Election interference

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 | Novembe 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 | PRINT

Terrorism

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

Money laundering

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

me new threats emerging. These

d external to the nation state.

Drug trafficking

Post Covid, corporates see huge increase in cyber crimes

Corruption

Fraud

Evidence on a computer system

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

ANY CRIME

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.

Medicrime

Hate crime

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

Kidnapping

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

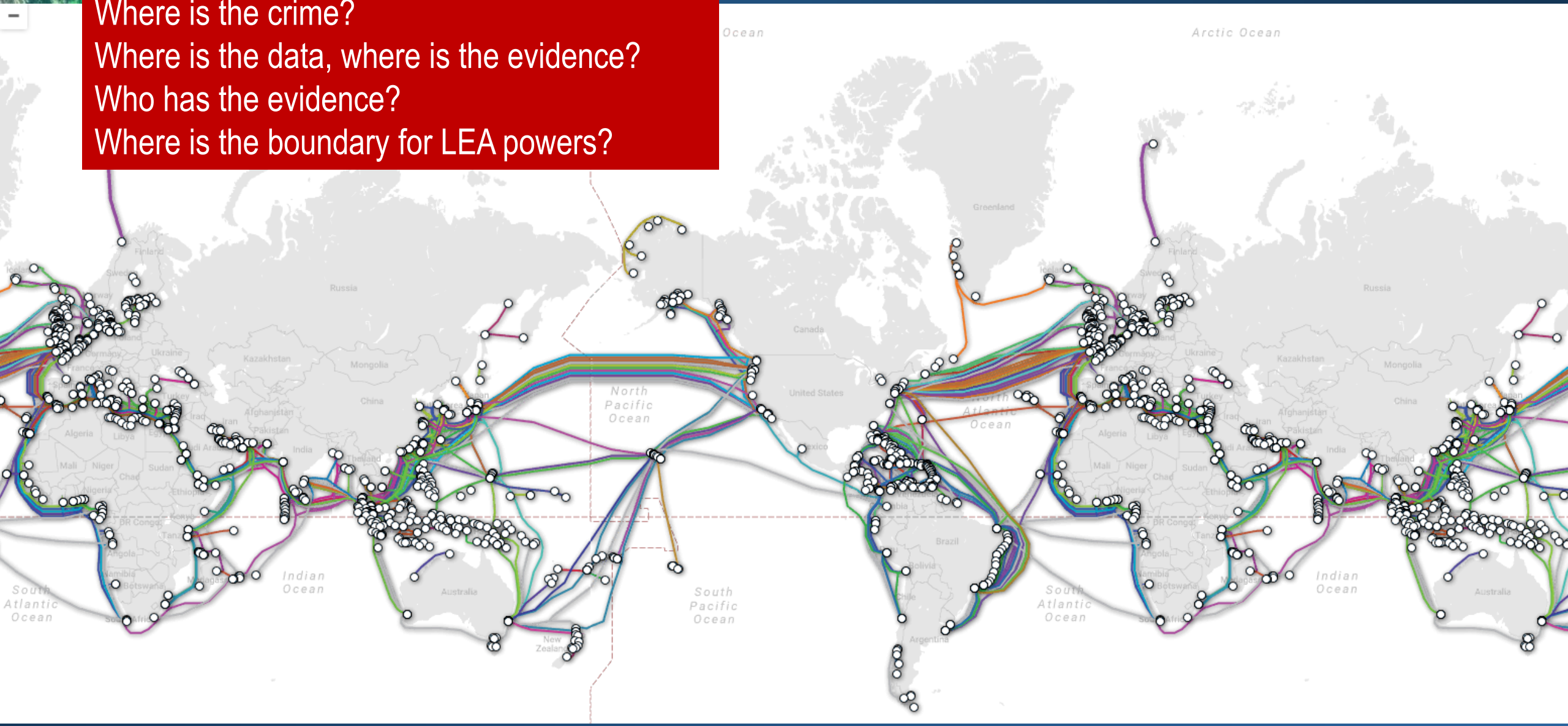
kney Borough Council have also been tight-lipped abou

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

Murder

Where is the evidence?

Where is the crime?
Where is the data, where is the evidence?
Who has the evidence?
Where is the boundary for LEA powers?



What we need

Cybercrime + e-evidence + transnational/ubiquitous nature of crime and evidence

- Need an effective criminal justice response

The mechanism of the Budapest Convention

Budapest Convention on Cybercrime (2001):

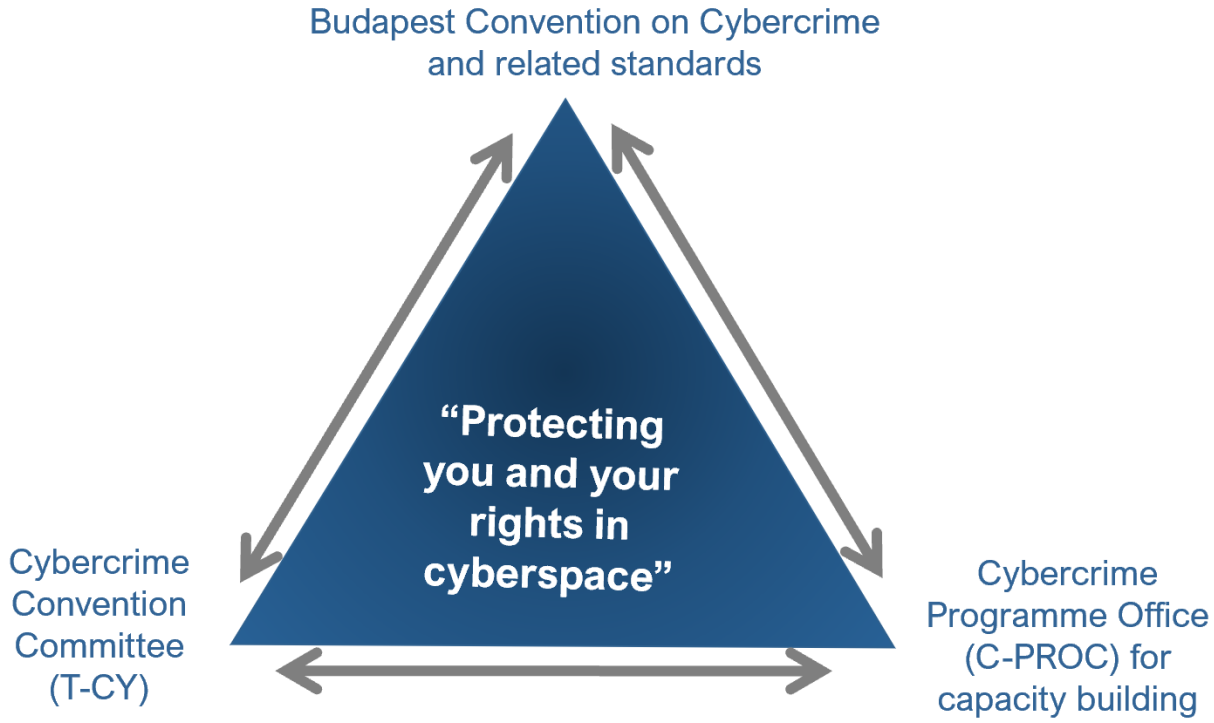
1. Specific offences against and by means of computer systems
2. Procedural powers with safeguards to investigate cybercrime and collect electronic evidence in relation to any crime
3. International cooperation on cybercrime and e-evidence

+ 1st Protocol on Xenophobia and Racism via Computer Systems

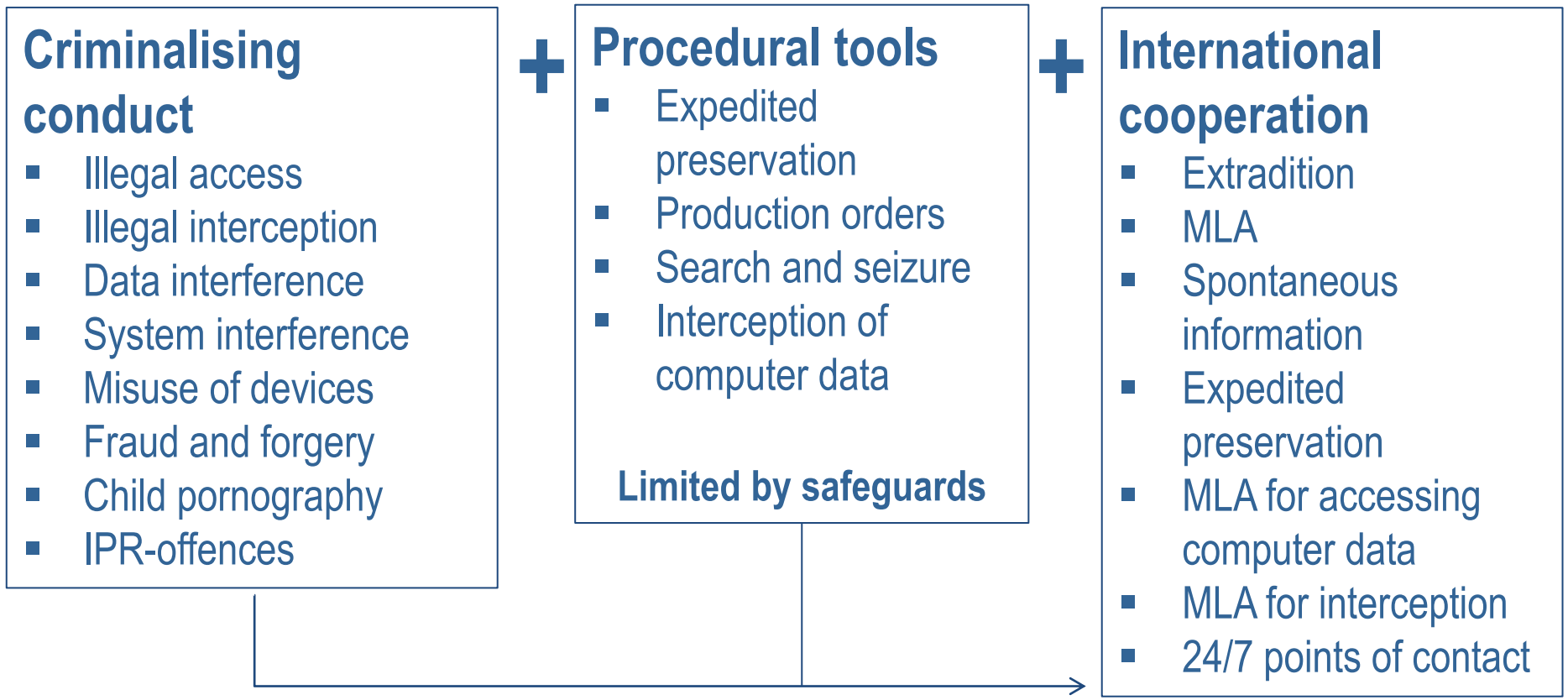
+ Guidance Notes

+ Protocol on enhanced cooperation on cybercrime and electronic evidence (opening for signature 12 May 2022 in Strasbourg)

By March 2022: 66 Parties and 14 Observer States

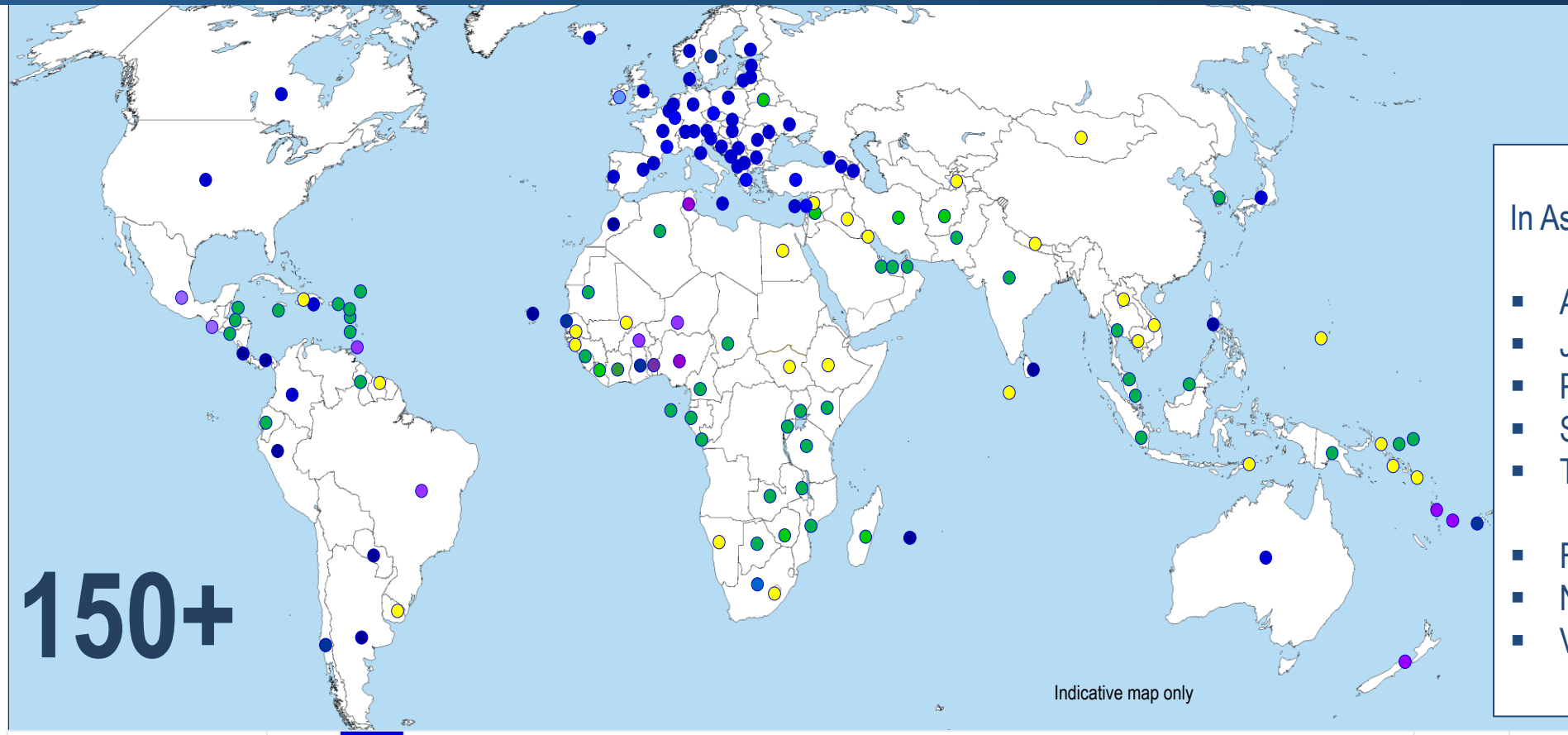


Content of the Budapest Convention



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

Reach of the Budapest Convention



In Asia/Pacific:

- Australia
- Japan
- Philippines
- Sri Lanka
- Tonga

- Fiji
- New Zealand
- Vanuatu

Parties:	66				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	12		Further States drawing on Budapest Convention for legislation:	30+	
=	**80**		=	**75+**	

Reach of the Budapest Convention

- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 14 signatories and States invited to accede
- ✓ 120+ States with substantive laws aligned with BC
- ✓ 150+ States have used it as a guideline or source
- ✓ 180+ States have been participating in COE activities on cybercrime
- ✓ Promoting rule of law and human rights in cyberspace

► **Instrument with global impact**

Treaty open for accession (article 37)

Phase 1:

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

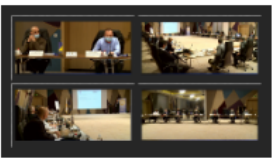
Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

The Budapest Convention: backed up by capacity building

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 38+ million
- 35 staff
- Some 400 activities per year
- Capacity for virtual capacity building
- Cooperation with 120+ countries in 2020/2021
- Joint projects with the European Union
- Voluntary contributions by Canada, Estonia, Japan, UK and USA in 2021/2
- Support to T-CY



iPROCEEDS-2: Cooperation between Internet Service Providers and Law Enforcement Agencies Implementation of Cyber Crime Investig

11 NOVEMBER 2020

Provided under the Joint Project of the European Un
the Ministry of Internal Affairs of Federation of Bosn
between Internet Service Providers and Law Enforce

CyberEast: W

12 NOVEMBER 2020

A new online event
Thursday, 12 Nover
women by including

Kiko's exciting

20 NOVEMBER 2020

The Council of Europ
(EndOCSEA@Europe)
character friend Kiko

GLACY+: CAB
Conference
during the C
Portuguese L

18 – 20 NOVEMBER 2020 | ONLINE | MULTIPLE COUNTRIES

The Presidency of Cape Verde of the Conference o

GLACY+: Web
towards a ne

9 NOVEMBER 2020

The webinar on "Ef
Budapest Convention", held on November 9th, 2020, was a joint initiative of the Cybercrime Programme Office (C-PROC) of the Council of Europe and the International Association of Prosecutors. During the 2 hours...

GLACY+: Judicial Trainers on Cybercrime and E-Evidence gather to discuss medium term development of a global network of

as held on the 17th of
meeting built on the results

eeting on the
dures (SOPs) and
Investigations and E-

nline national meeting on the
ercrime Investigations and E-

ybercrime legislation

estigators took part in the
essionals of justice, co-

cts of COVID-19 on

uncil of Europe teamed up on
cybercrime in the Pacific. The
event gathered more than 50 cybercrime policy makers, criminal justice and law...

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

What crime?

Who did it?

What evidence?

COVID-19 and the Budapest Convention

COVID-19 related crime in cyberspace

- Phishing campaigns and malware distribution through seemingly genuine information or advice on COVID-19 .
- Ransomware shutting down medical, scientific or other health-related facilities testing for COVID-19 or developing vaccines
- Ransomware targeting individuals through apps claiming to provide genuine information on COVID-19
- Attacks against critical infrastructures or international organizations
- Offenders targeting employees who are teleworking
- Fraud schemes offering personal protective equipment or fake medicines claiming to prevent or cure SARS-CoV-2
- Misinformation or fake news to create panic, social instability, xenophobia, racism or distrust in measures taken health authorities

Budapest Convention – Articles

- 2 – Illegal access
- 3 – Illegal interception
- 4 – Data interference
- 5 – System interference
- 6 – Misuse of devices
- 7 – Forgery
- 8 – Fraud
- 10 – IPR offences

Protocol on Xenophobia and Racism

Guidance Notes on

- Botnets
- DDOS attacks
- Critical information infrastructure attacks
- Malware
- Spam
- ID theft

Procedural powers to secure evidence and identify offenders

- 16+17 – Expedited preservation
- 18 – Production orders
- 19 – Search and seizure
- 20+21 – Interception

With safeguards

- Article 15

Guidance Note on

- Article 18 – Production orders

Framework for international cooperation

- Articles 23 - 35

The tools of the Budapest Convention (criminalization, procedural powers, international cooperation)

Backed up capacity building programmes

Are available to address COVID-19 related cybercrime … and similar future crises.

Coming soon (12 May 2022):

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

- Direct requests to registrars for disclosure of WHOIS information
- Direct orders to 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

(Details will follow in another session of this workshop)