EUROPEAN CONFERENCE OF PROSECUTORS

ENHANCED CO-OPERATION AND DISCLOSURE OF ELECTRONIC EVIDENCE ADDED VALUE OF THE BUDAPEST CONVENTION AND ITS SECOND ADDITIONAL PROTOCOL – MUTUAL TRUST AS A PRECONDITION

Palermo, 6 May 2022

Ioana Albani, T-CY member, Romania
prosecutor at the Directorate for Investigating Organized Crime and Terrorism (DIICOT)

The problem of cybercrime …
… and e-evidence re all types of crime

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

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

Profile
INTRUSION In

Subscribe

Subscribe

SECURITY

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

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

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 - 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

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.

By Danny Palmer | November 20, 2020 -- 12:40 GMT (12:40 GMT) |
Topic: Security

MORE FROM DANNY PALMER

Secu
Scar

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.

Warning: Domestic cyber terrorism on the rise in 2021

SPECIAL

LISTEN | PRIN

attempt to re-build for 2021, next year
ome new threats emerging. These
nd

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

News, World

Covid-19 lockdowns drive spike in online child abuse

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

Out-of-school kids and adult predators spending more time at home and on the internet during the coronavirus pandemic is the "perfect storm" driving a spike in online child sex

Post Covid, corporates see huge increase in cyber crimes

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

yber-attack, which I covered in a blog post titled The Multi-Milli
ovided few details about their cyber-attack which has been
e UK media are widely reporting United's leaky IT defences was
on's Hackney Borough Council have also been tight-lipped abou
pacted its service delivery to Londoners. Like United, this attack

The response: **The mechanism of the Budapest Convention**

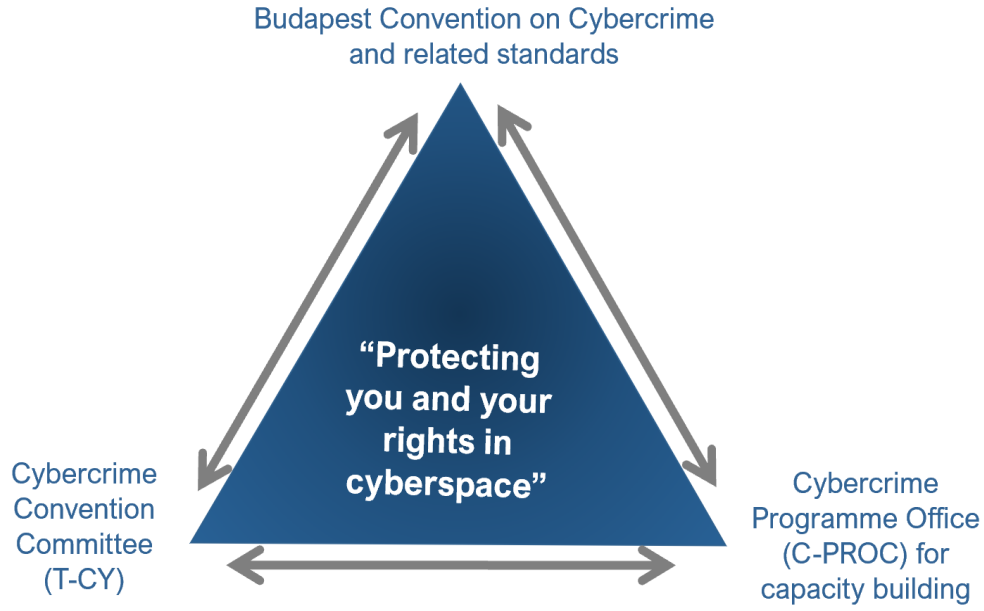
Budapest Convention on Cybercrime (2001):

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

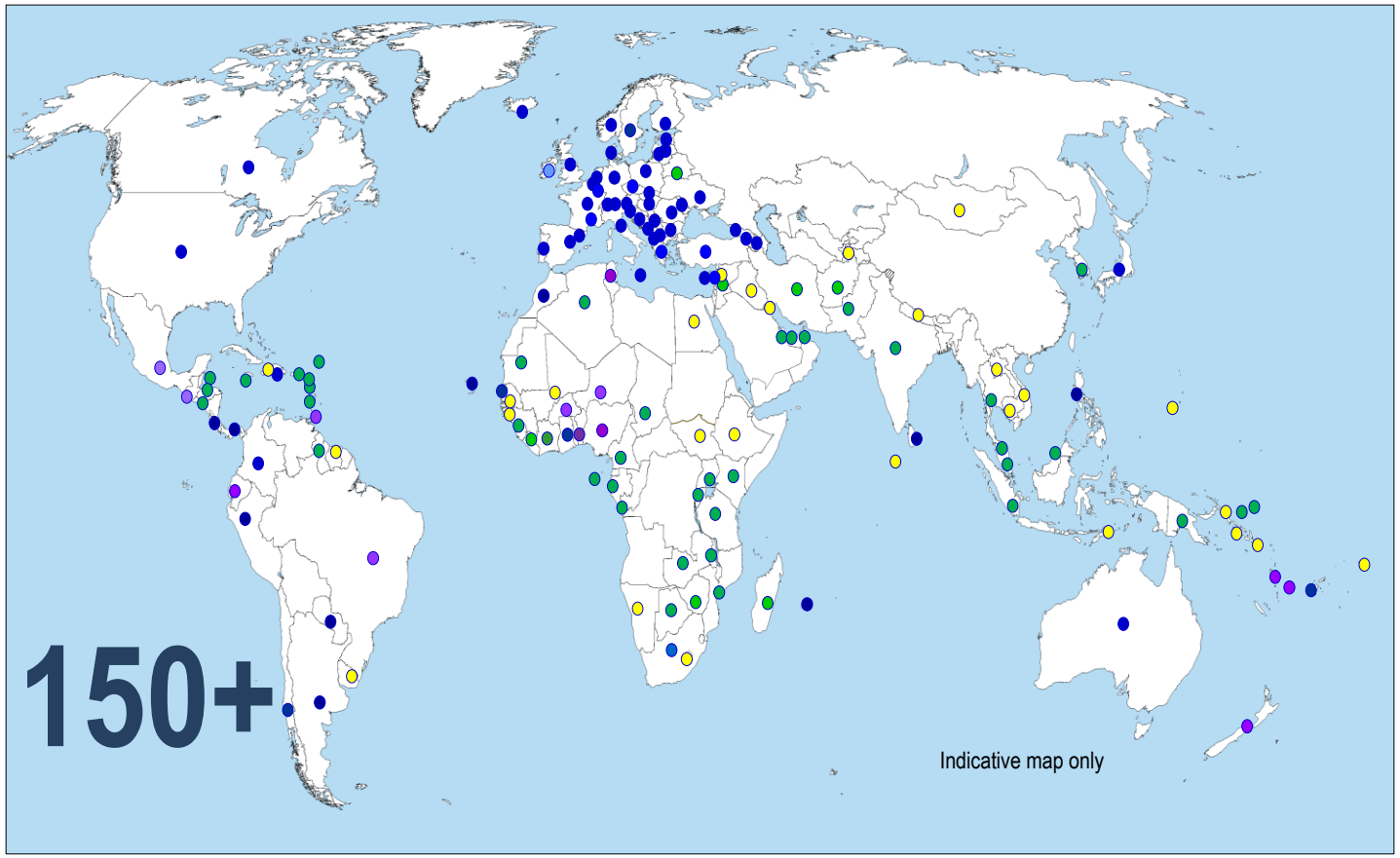
+ Guidance Notes

+ 2nd Protocol on enhanced cooperation on cybercrime and electronic evidence adopted 17 Nov 2021



Reach of the Budapest Convention

- ✓ 20 years of Budapest Convention (2001-2021): global impact
- ✓ 66 Parties + 2 signatories + 13 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



► **Multilateral instrument – the same expected from 2nd Protocol**

The 2nd Additional Protocol to the Convention on Cybercrime: the process of negotiations

Protocol:

- Prepared by Protocol Drafting Plenary and Drafting Groups established by the Cybercrime Convention Committee September 2017 to May 2021
- 91 sessions of the PDP, PDG and PDG subgroups
- 75 States and several international organisations participated with over 620 experts
- Data protection experts participated in negotiations
- 6 rounds of stakeholder consultations

Formally adopted on 17 November 2021

Carefully calibrated text designed to be consistent with the acquis of the Council of Europe but also to meet the requirements of all other Parties to the Budapest Convention

May 2022, Council of Europe, Strasbourg:

12 May 2022 - Opening for signature of the Second Additional Protocol

13 May 2022 - Conference on enhanced cooperation and disclosure of electronic evidence

2nd 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

Example: Direct cooperation with entities in other Parties

Issue: no basis for direct cooperation

Current practices:

- Limited information publicly offered/available due to data protection rules
- MLA

Article 6 – Request for domain name registration information

OBJECTIVE – to set legal basis and provide procedure for (**voluntary**) **direct cooperation** between the competent authorities of one Party and an entity providing domain name registration in the territory of another Party

LIMITED SCOPE – specific criminal investigation or proceeding (concerning criminal offences related to computer systems and data and to the collection of evidence in electronic form of a criminal offence) **for information for identifying or contacting the registrant of a domain name**

Example: Direct cooperation with service providers in other Parties

Issue: Voluntary disclosure [of subscriber information] by service providers

Current practices:

- More than 200,000 requests/year by BC Parties/Observers to major US providers
- Disclosure of subscriber information (ca. 64%)
- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No admissibility of data received in some States

Article 7 - Disclosure of subscriber information

OBJECTIVE – to set legal basis and provide procedure for **direct cooperation** between the **competent authorities** of one Party and **a service provider** in the territory of another Party, which has possession of control of the data sought.

LIMITED SCOPE – specific criminal investigation or proceeding (concerning criminal offences related to computer systems and data and to the collection of evidence in electronic form of a criminal offence) and **only** for specified stored **subscriber information** that is **needed** for a specific investigation

Example: Giving effect to orders from another party for expedited production of data

Issue: the sensitive nature of the traffic data/ different interpretation re dynamic/static IP, log in IP)

Current practices:

- Providers decide whether to respond to lawful requests and to notify customers
- Provider policies/practices volatile
- Data protection concerns
- No admissibility of data received in some States

Article 8 – "Giving effect

OBJECTIVE – <u>compelling mechanism to produce data</u> upon an order issued by authorities in another Party, as a part of a request **(a simplified procedure of conversion of an order issued in another Party into an enforceable order under a mechanism provided by the domestic law of the requested Party)**

LIMITED SCOPE – a. production of stored **subscriber information or traffic data** that **is needed** in a specific criminal investigation or proceeding. **b. specific enforcement mechanism for orders issued under Article 7**

Example: Cooperation in an emergency situation

Issue: no common understanding on "emergency", thus lack of predictability in providing responsive approaches in such cases

Article 3 – Definitions

…

2.c. For the purposes of this Protocol, the following additional definitions apply: an "**emergency**" means **a situation in which there is a significant and imminent risk to the life or safety of any natural person;**

Examples:

Hostage situations, kidnappings, ongoing sexual abuse of a child, anticipated terrorist attack, cyber attacks on critical infrastructure resulting in imminent death or injury.

- **Article 9 - Expedited disclosure of stored computer data in an emergency**
- **Article 10 - Emergency mutual assistance**

2nd Additional Protocol to the Convention on Cybercrime: content / example

Article 10

OBJECTIVE - to provide legal basis for a maximally expedited procedure for **mutual assistance requests** made in emergency situations

NOT LIMITED to stored evidence in a service provider's possession or control in the territory of another Party

Mandatory content - a description of the facts that demonstrate that there is an emergency and how the assistance sought relates to it

Option for a Party to declare the 24/7 Point of Contact as channel of transmission

Article 9

OBJECTIVE – legal basis for obtaining immediate assistance for expedited disclosure of **specified, stored computer data without a request for mutual assistance.**

LIMITED to specified stored computer data in a service provider's possession or control in the territory of another Party

Standard content

Procedural measure to enable the **24/7 Point of Contact to transmit a request to and receive a request from a 24/7 Point of Contact** in another Party seeking immediate assistance

LIMITED to emergency situations as defined

2nd Additional Protocol to the Convention on Cybercrime: content / example

Issue: Efficiency versus 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, a notification mechanism to permit domestic safeguards and limit information to be provided

2nd Additional Protocol to the Convention on Cybercrime: benefits

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)

THANK YOU!

Ioana Albani
Prosecutor
albani_ioana@mpublic.ro