INSTITUT DES HAUTES ÉTUDES DE DÉFENSE NATIONALE
Session cybersécurité, Webinar, 16 novembre 2022, 17h30-19h00

Réponses internationales aux défis de la cybercriminalité et des preuves électroniques:

La Convention sur la cybercriminalité et le deuxième protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques

Alexander Seger
Division Cybercriminalité
Conseil de l'Europe

www.coe.int/cybercrime

1

Le problème de la cybercriminalité …

Cybercrime To Cost The World $10.5 Trillion Annually By 2025

Every U.S. business is under cyberattack

SECURITY

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

Par Sophy Caulier

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.

Warning: Domestic cyber terrorism on the rise in 2021

SPECIAL

BY TIM SANDLE NOV 25, 2020 IN BUSINESS

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.

News, World

Covid-19 lockdowns drive spike in online child abuse

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

Post Covid, corporate

US issues rare security alert as Montenegro battles ongoing ransomware attack

40% Increase in Ransomware Attacks in Q3 2020

by saptarshi das on November 16, 2020

40% increase in Ransomware Attacks in Q3 2020

CYBER BULLYING

DNA Exclusive: Women soft target of cyberbullying online violence on social media

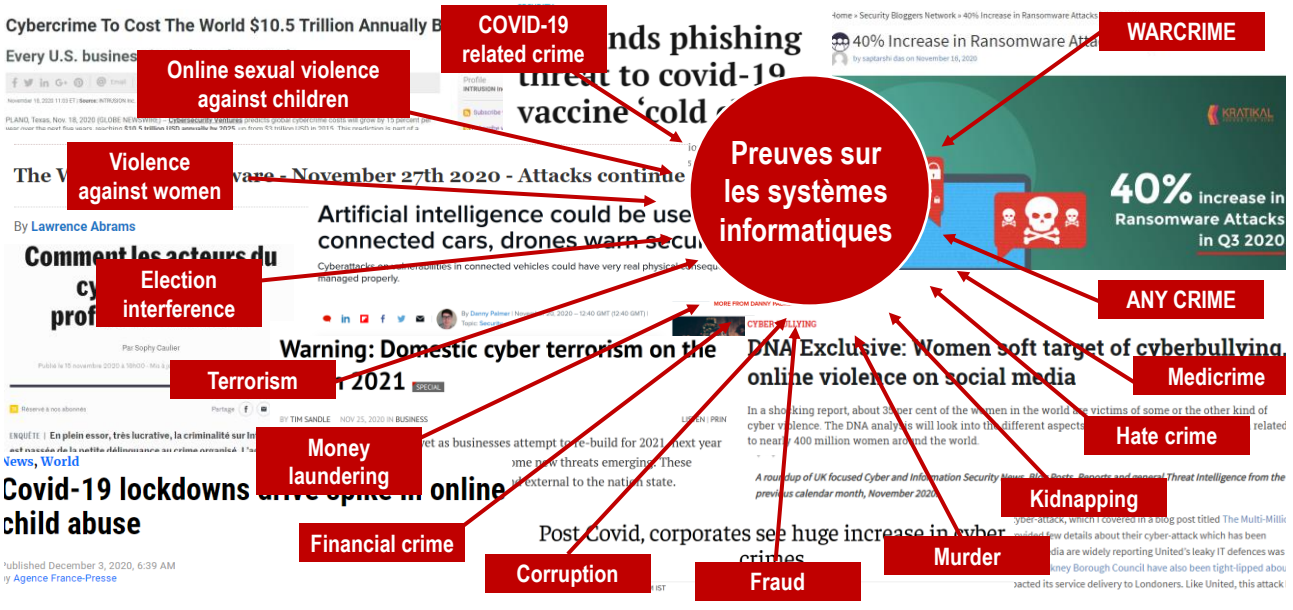
In a shocking report, about 35 per cent of the women in the world are victims of some or the other kind of cyber violence. The DNA analysis will look into the different aspects of cyber violence against women relate to nearly 400 million women around the world.

Costa Rica's 'War' Against Ransomware Is a Wake-Up Call for the Region

James Bosworth Jul 18, 2022

2

… et preuves électroniques concernant tous les types de crimes



3

Le mécanisme de la convention sur la cybercriminalité

Convention de Budapest sur la cybercriminalité (2001) :

- Infractions spécifiques contre et au moyen de systèmes informatiques
- Pouvoirs procéduraux assortis de garanties pour enquêter sur la cybercriminalité et recueillir des preuves électroniques en rapport avec tout crime
- Coopération internationale sur la cybercriminalité et les preuves électroniques

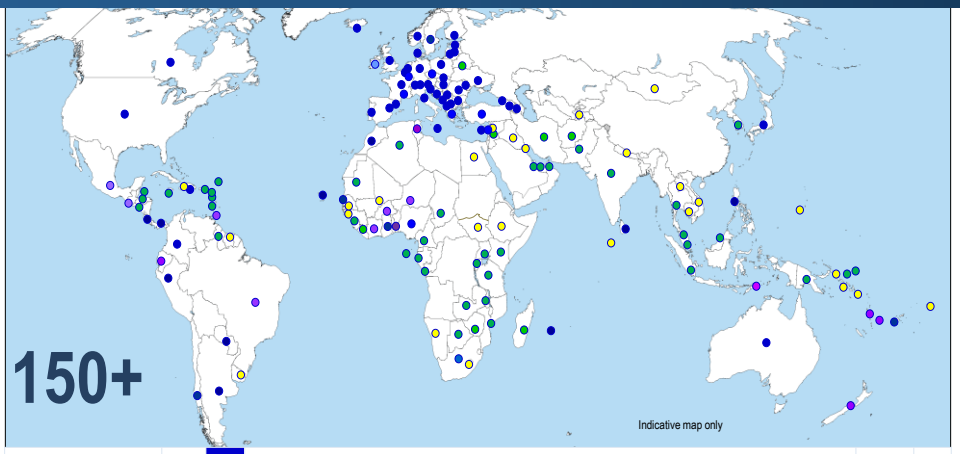
+ 1ier Protocole sur la xénophobie et le racisme via les systèmes informatiques

+ Notes d'orientation

+ 2ième protocole additionnel relatif au renforcement de la coopération et de la divulgation de preuves électroniques
(ouvert à la signature 12 mai 2022)

4

Portée géographique de la Convention sur la cybercriminalité



Parties:	67				
Signed:	2		Other States with substantive laws broadly in line with Budapest Convention:	45+	
Invited to accede:	14		Further States drawing on Budapest Convention for legislation:	30+	
=	**83**		=	**75+**	

5

La Convention de Budapest: structure et contenu

Droit pénal matériel

- Accès illégal
- Interception illégale
- Atteinte à l'intégrité des données
- Atteinte à l'intégrité du système
- Abus de dispositifs
- Falsification informatique
- Fraude informatique
- Pornographie infantile
- Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

+

Droit procédural

- Conservation rapide de données
- Injonction de produire
- Perquisition et saisie de données
- Interception des données relatives au contenu
- Limitée par des garanties

+

Coopération internationale

- Extradition
- MLA
- Informations spontanées
- Conservation rapide
- MLA pour l'accès aux données informatiques
- MLA pour l'interception
- Des points de contact 24 heures sur 24, 7 jours sur 7

Harmonisation

Pouvoirs procéduraux et coopération internationale pour toute infraction pénale impliquant des preuves sur un système informatique !

www.coe.int/cybercrime

6

La Convention sur la cybercriminalité : soutenue par le renforcement des capacités

GLACY+ and Octopus Project: Workshop on countering online child sexual exploitation and abuse, Mauritius

MAURITIUS | 26-27 OCTOBER 2022

The increasing use by children of information and communication technologies (ICTs), such as...

Strengthening international cooperation on cybercrime and electronic evidence in the Americas

SAN JOSÉ, COSTA RICA | 7 NOVEMBER 2022

Efficient international cooperation has never been more important in enabling an effective and...

CyberEast: Fourth Regional Cyber Cooperation Exercise

13 - 16 SEPTEMBER 2022 | ISTANBUL, TÜRKIYE

In the world of today, the increasing number of attacks against computer systems and data is a growing concern for both cyber security professionals and criminal justice authorities. This is the reason why the CyberEast and CyberSecurity EAST projects, co-funded by the European Union, seek to...

GLACY+: Supporting national delivery of an introductory course on cybercrime and electronic evidence in Benin

2 SEPTEMBRE 2022 | COTONOU, BENIN

GLACY+ and INTERPOL: ECOWAS trainers participated in a Training-of-Trainers of the First Responders course on e-evidence

20 JUNE - 29 JULY 2022 | ONLINE AND CABO VERDE

More action needed to promote the role of women in the fight against cybercrime

SAN JOSÉ, COSTA RICA | 10 NOVEMBER 2022

Women have a crucial role to play in effective criminal justice responses to cybercrime, stated...

Council of Europe and EUROJUST: Cooperation on ransomware

THE HAGUE, NETHERLANDS | 3-4 NOVEMBER 2022

On 3 and 4 November, the Cybercrime Programme Office of the Council of Europe and EUROJUST...

7

La Convention sur la cybercriminalité : soutenue par le renforcement des capacités

Bureau du programme de lutte contre la cybercriminalité du Conseil de l'Europe (C-PROC) en Roumanie :

- Soutenir les processus de changement vers des capacités de justice pénale renforcées en matière de cybercriminalité et de preuves électroniques conformément à la Convention de Budapest et aux garanties de l'état de droit
- 5 projets en cours avec un budget cumulé de 38+ millions d'euros
- 38 employés
- Quelque 400 activités par an
- Capacité de renforcement des capacités virtuelles
- Coopération avec plus de 120 pays en 2021/2022Projets conjoints avec l'Union européenne
- Contributions volontaires du Canada, de la Hongrie, de l'Italie, du Japon, du Royaume-Uni et des États-Unis en 2021/2
- Soutien au T-CY

Projets actuels:

- GLACY+
- CyberEast
- CyberSouth
- iPROCEEDS-2
- Octopus

8

Pourquoi un nouveau protocole?

Cybercriminalité : menace de

- Droits humains
- La démocratie
- État de droit loi

Obligations positives :

- Mettre en place les moyens de protéger les droits des individus, également contre la criminalité

Problème:

- Prolifération de la cybercriminalité
- Tout type de crime impliquant désormais des preuves électroniques
- Preuve quelque part dans des juridictions étrangères, multiples, changeantes ou inconnues
- Moyens efficaces non disponibles pour obtenir la divulgation des preuves électroniques
- Moins de 0,1 % des infractions dans le cyberespace donnent lieu à des poursuites et à des condamnations
- Les victimes obtiennent-elles justice?

2e protocole pour aider à relever ces défis

Pourquoi un nouveau protocole?

Défis spécifiques

- Comment obtenir efficacement les informations des abonnés?
- Comment coopérer directement avec un fournisseur de services dans une autre partie?
- Comment obtenir WHOIS (informations d'enregistrement de nom de domaine) auprès des bureaux d'enregistrement?
- Comment obtenir des données stockées, y compris du contenu, dans une situation d'extrême urgence?
- Comment rendre l'entraide plus efficace?
- Comment concilier des mesures efficaces et efficientes avec l'état de droit et les exigences en matière de protection des données?

Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques: contenu

Préambule

Chapitre I - Dispositions communes

Article 1 – But
Article 2 – Champ d'application
Article 3 – Définitions
Article 4 – Langue

Chapitre II - Mesures de coopération renforcée

Section 1 – Principes généraux applicables au chapitre II

Article 5 – Principes généraux applicables au chapitre II

Section 2 – Procédures renforçant la coopération directe avec les fournisseurs et les entités dans les autres Parties

Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine
Article 7 – Divulgation directe de données relatives aux abonnés

Section 3 – Procédures renforçant la coopération internationale entre autorités pour la divulgation de données informatiques stockées

Article 8 – Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic
Article 9 – Divulgation accélérée de données informatiques stockées en situation d'urgence

Section 4 – Procédures relatives à la demande d'entraide urgente

Article 10 – Demande d'entraide urgente

Section 5 – Procédures relatives à la coopération internationale en l'absence d'accords internationaux applicables

Article 11 – Vidéoconférence
Article 12 – Équipes communes d'enquête et enquêtes communes

Chapitre III – Conditions et garanties

Article 13 – Conditions et garanties
Article 14 – Protection des données à caractère personnel

Chapitre IV – Dispositions finales

Article 15 – Effets de ce Protocole
Article 16 – Signature et entrée en vigueur
Article 17 – Clause fédérale
Article 18 – Application territoriale
Article 19 – Réserves et déclarations
Article 20 – Statut et retrait des réserves
Article 21 – Amendements
Article 22 – Règlement des différends
Article 23 – Consultations des Parties et évaluation de la mise en œuvre
Article 24 – Dénonciation
Article 25 – Notification

11

Deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques: contenu

- **Article 6 – Demande d'informations concernant l'enregistrement d'un nom de domaine** (WHOIS) ► Demande directe au registraire d'une autre partie
- **Article 7 – Divulgation directe de données relatives aux abonnés** ► Injonction directe au fournisseur d'une autre partie
- **Article 8 – Donner effet aux injonctions ordonnant la production accélérée de données** ► Gouv-à-gouv mais pas (nécessairement) entraide judiciaire
- **Article 9 – Divulgation accélérée de données informatiques stockées en situation d'urgence** ► Gouv-à-gouv via point de contact 24/7 (pas entraide judiciaire)
- **Article 10 – Demandes d'entraide judiciaire urgentes** (emergency)
- **Article 11 – Vidéoconférence** ► Entraide judiciaire (gouv-à-gouv)
- **Article 12 – Équipes communes d'enquête et enquêtes communes** ► Entraide judiciaire (gouv-à-gouv)
- **Article 13 – Conditions et sauveguardes**
- **Article 14 – Garanties de protection des données**

12

Deuxième Protocole additionnel à la Convention sur la cybercriminalité: prochaines étapes

Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques (STCE n° 224)

Signatures (situation 15 nov 2022):

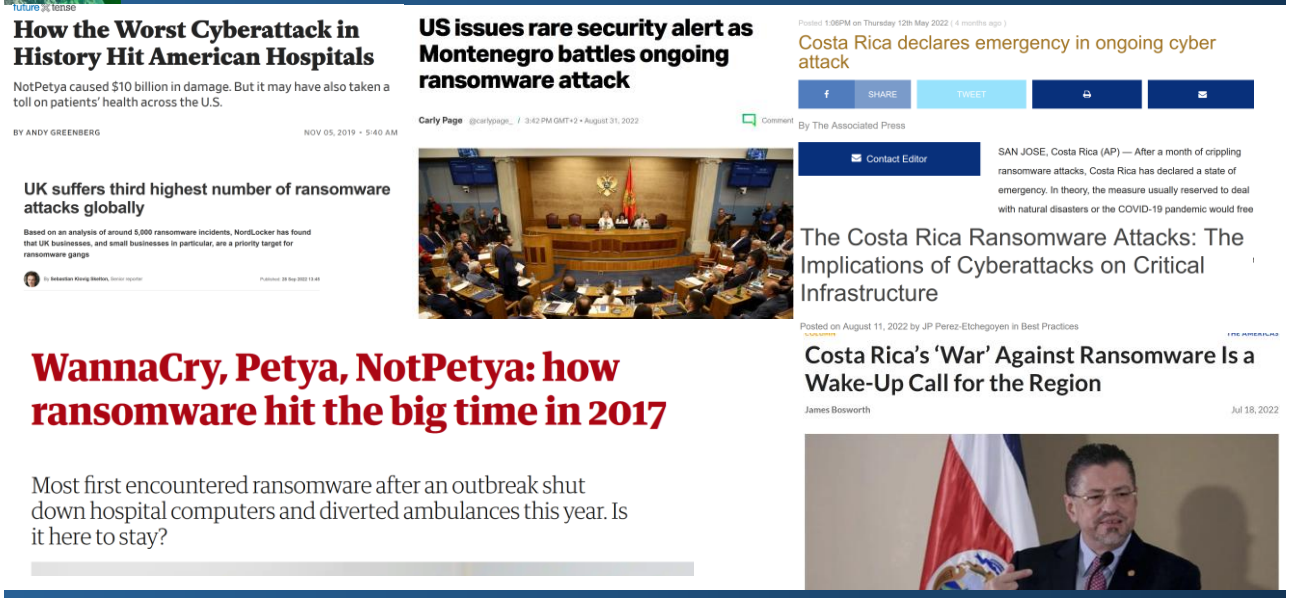
1. Andorra
2. Austria
3. Belgium
4. Bulgaria
5. Chile
6. Colombia
7. Costa Rica
8. Estonia
9. Finland
10. Iceland
11. Italy
12. Japan
13. Lithuania
14. Luxembourg
15. Montenegro
16. Morocco
17. Netherlands
18. North Macedonia
19. Portugal
20. Romania
21. Serbia
22. Spain
23. Sweden
24. USA

Prochaines étapes:

- ► Signature par les autres Parties
- ► Ratification (5 nécessaires pour l'entrée en vigueur)
- ► Renforcement des capacités

13

La Convention (avec les Protocoles) couvre-t-elle les infractions liées aux rançongiciels ?



14

Contenu de la Convention de Budapest : exemple de rançongiciel

Article	Convention sur la cybercriminalité
Art. 2	Accès illégal
Art. 3	Interception illégale
Art. 4	Atteinte à l'intégrité des données
Art. 5	Atteinte à l'intégrité du système
Art. 6	Abus de dispositifs
Art. 7	Falsification informatique
Art. 8	Fraude informatique
Art. 11	Tentative et complicité
Art. 12	Responsabilité des personnes morales
Art. 13	Sanctions et mesures

Article	Convention sur la cybercriminalité
Art. 14-21	Pouvoirs procéduraux

Infractions liées aux rançongiciels

Article	Convention sur la cybercriminalité
Art. 23-35	Coopération internationale

Article	2ème protocole
Art. 7	Article 7 – Divulgation de données relatives aux abonnés
Art. 8	Donner effet aux injonctions d'une autre Partie ordonnant la production accélérée de données relatives aux informations sur les abonnés et au trafic
Art. 9	Divulgation accélérée de données informatiques stockées en situation d'urgence
Art. 10	Demande d'entraide urgente
Art. 11	Vidéoconférence
Art. 12	Équipes communes d'enquête et enquêtes communes

15

Conclusions

- La Convention de Budapest - avec son 2e Protocole - restera probablement la norme internationale la plus pertinente en matière de cybercriminalité en matière de justice pénale
- Les dispositions de ce protocole seront utiles sur le plan opérationnel et politique
- Mesures efficaces pour enquêter et sécuriser les preuves électroniques avec les protections de l'état de droit et des garanties de protection des données
- Avec ce protocole, la Convention de Budapest continuera à défendre un Internet libre et ouvert où les gouvernements s'acquittent de leur obligation de protéger les individus et leurs droits dans le cyberespace en même temps.
- ≠ surveillance de masse, ≠ collecte massive de données, ≠ contrôle gouvernemental de l'information

www.coe.int/cybercrime

16

17