

La coopération internationale contre la cybercriminalité: stratégies et défis

Alexander Seger

Secrétaire exécutif du Comité de la Convention sur la Cybercriminalité
Conseil de l'Europe

Atelier de

Concertation sur l'Adhésion de la République Islamique de Mauritanie à la Convention de Budapest sur la Cybercriminalité

organisé par le Gouvernement mauritanien représenté par le Ministère de l'Emploi, de la Formation
Professionnelle et des TIC et le Conseil de l'Europe
Nouakchott, 9-10 mars 2015, Hôtel Mauricenter



Ministère de l'Emploi, de la Formation
Professionnelle et des Technologies de
l'Information et la Communication

COUNCIL OF EUROPE



CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Cybercriminalité v. cybersecurité: quelle différence?

Cybercriminalité v. cybersecurité

Stratégies de la Cybersecurité

Securité, résilience, confiance,
fiabilité de TIC

incidents de sécurité
non-intentionnels

Sinistres

Défaillance technique

Défaillance humaine

Attaques intentionnelles
contre les TIC par

Acteurs état- Acteurs non- Terror- Crimin-
iques étatiques istes els

Attaques
contre
infrastructure
critique

Autres attaques
contre la
confidentialité,
l'intégrité et la
disponibilité des
TIC

Cybercrime stratégies contre la cybercriminalité

Etat de droit/ justice pénale et
droit de l'homme

Infractions
par TIC

Infractions
impliquant
des TIC

Fraude,
Exploit.
Enfants,
Terrorisme par
TIC, IPR
Extortion, etc

Toutes
infractions
impliquant
preuves
électron.



Elements d'une stratégie contre la cybercriminalité

Objectif

Protection contre:

- **Les attaques intentionnelles contre et par les TIC**
- **Toutes infractions impliquant les preuves électroniques**

- **Systemes de signalement**
- **Prévention**
- **Législation, incl. garanties et protection des données**
- **Unités spécialisées**
- **Coopération interinstitutionnelle**
- **Formation policière**
- **Formation judiciaire**
- **Coopération public/privé**
- **Coopération internationale efficace**
- **Investigations financières, prévention de fraude and blanchiment d'argent**
- **Protection des enfants**

Programmes de coopération pour la mise en œuvre de stratégies contre la cybercriminalité

- ▶ **C-PROC (Bureau de programme du Conseil de l'Europe sur la cybercriminalité, à Bucarest, Roumanie)**



GLACY

Global Action on Cybercrime
Action globale sur la cybercriminalité

Funded
by the European Union
and the Council of Europe



COUNCIL OF EUROPE



Implemented
by the Council of Europe

EU/COE Joint Project on Global Action on Cybercrime *Projet joint UE/CdE Action globale sur la cybercriminalité*

Duration/durée: 36 months/*mois* (Nov 2013 – Oct 2016)

Budget: EUR 3.35 million

Funding: European Union (Instrument for Stability, IfS) and
Council of Europe

Financement: Union européenne et Conseil de l'Europe

Défis de la coopération internationale



Défis de la coopération internationale



scène de crime



La Convention de Budapest

Convention de Budapest

Article 23 – Principes généraux relatifs à la coopération internationale

Article 24, 25, 26, 27

Article 29 – Conservation rapide de données informatiques stockées

Article 30 – Divulgence rapide de données conservées

Article 31 – Entraide concernant l'accès aux données stockées

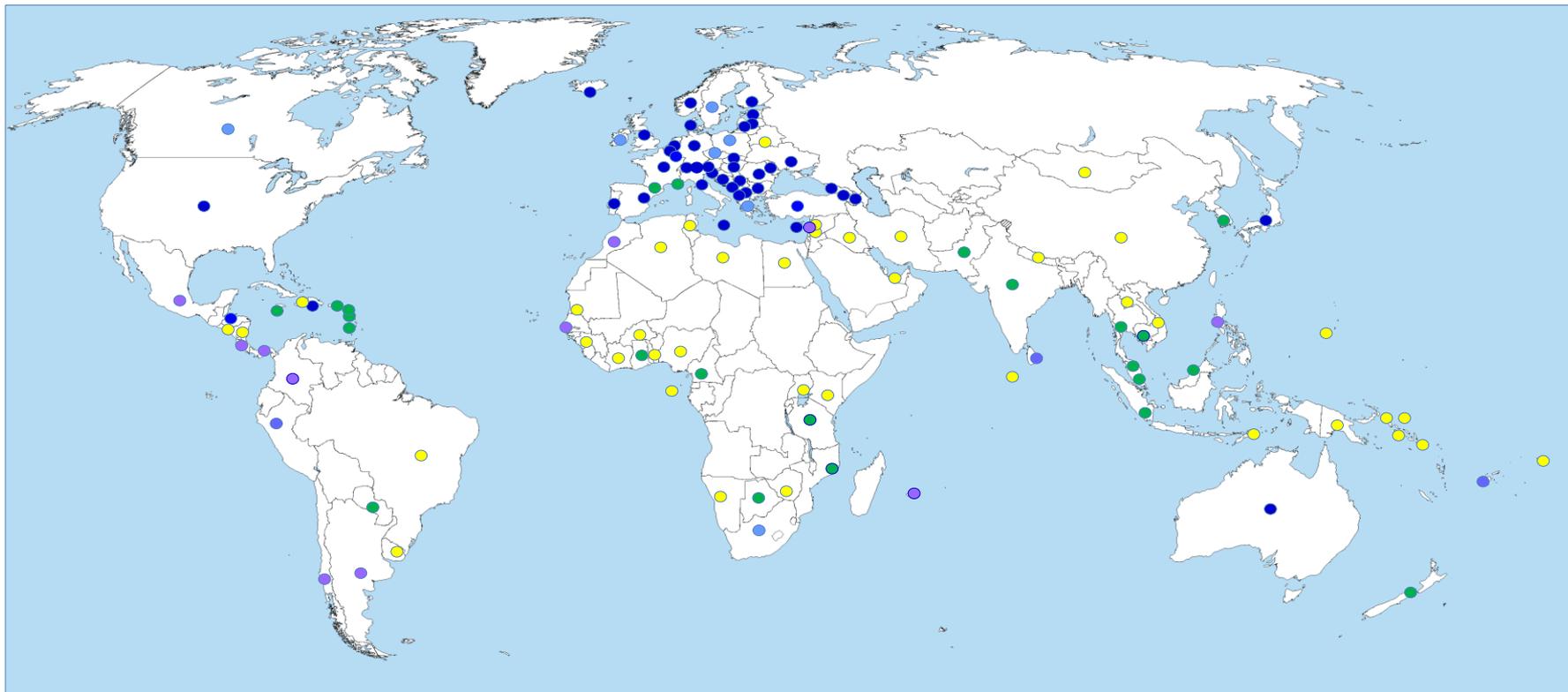
Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

Article 34 – Entraide en matière d'interception de données relatives au contenu

Article 35 – Réseau 24/7

Etats faisant usage de la Convention de Budapest

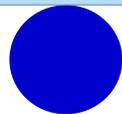


Ratific./adhésions: 45

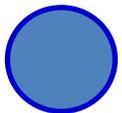
Signatures: 8

Invités à adhérer: 12

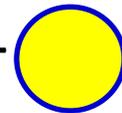
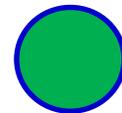
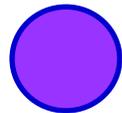
= 65



Etats avec (projets de) lois fondés sur la Convention de Budapest= 20



Autres Etats utilisant la Convention= 45+



Analyse du Comité de la Convention sur la Cybercriminalité (T-CY) 2014

- ▶ **Evaluation des dispositions de la Convention de Budapest sur la cybercriminalité concernant l'entraide judiciaire**

Résultats de l'évaluation

- **Le processus de demande d'entraide judiciaire (DEJ) est jugé inefficace en général, et en particulier pour ce qui concerne l'obtention de preuves électroniques.**
- **les Parties semblent ne pas mettre pleinement à profit les opportunités offertes par la Convention de Budapest sur la cybercriminalité et par d'autres accords afin de parvenir à une entraide efficace en matière de cybercriminalité et de preuves électroniques**

Résultats de l'évaluation

- Pour ce qui est du type d'informations demandées, les informations concernant les abonnés ressortent comme étant les informations les plus fréquemment demandées.

Types d'informations demandés

- 1. Informations relatives aux abonnés (80+%?)**
- 2. Données de trafic**
- 3. Données de contenu**

Infractions sous-jacentes:

- 1. Fraudes et autres criminalités financières**
- 2. Crimes graves et violents (meurtre, agressions, traites, maltraitements des enfants etc.)**
- 3. Infractions contre les systèmes informatiques**

Résultats de l'évaluation ► Recommandations

- **Mettre en œuvre et appliquer pleinement les dispositions de la Convention de Budapest sur la cybercriminalité, y compris les pouvoirs en matière de conservation (suite au rapport d'évaluation de 2012 du T-CY).**
- **Envisager de tenir des statistiques ou d'établir d'autres mécanismes pour suivre l'efficacité du processus d'entraide en ce qui concerne la cybercriminalité et les preuves électroniques.**
- **Envisager, pour l'entraide, d'affecter davantage de personnel et du personnel plus formé aux technologies,**
- **Envisager de dispenser une meilleure formation pour renforcer l'entraide, la coopération policière et d'autres formes de coopération internationale en matière de cybercriminalité et de preuves électroniques.**
- **Renforcer le rôle des points de contact 24/7 conformément à l'article 35 Convention de Budapest**

Résultats de l'évaluation ► Recommandations

- **Considérer la rationalisation des procédures et réduire le nombre d'étapes requises pour les demandes d'entraide au niveau national. A cet égard Les Parties doivent partager les bonnes pratiques avec le T-CY.**
- **Les Parties devraient utiliser tous les canaux disponibles pour la coopération internationale. Ceci peut inclure l'entraide judiciaire formelle, la coopération policière et d'autres.**
- **Etablir des procédures d'urgence pour les demandes liées aux risques pour la vie et à des circonstances extrêmes similaires. Le T-CY devrait documenter les pratiques des Parties et des fournisseurs de service.**
- **Confirmer la réception des demandes systématiquement et notifier les actions prises**

Résultats de l'évaluation ► Recommandations

Les recommandations qui devraient être prises en charge à travers un Protocole additionnel à la Convention de Budapest sur la Cybercriminalité

- **Permettre – via des amendements juridiques nationaux et accord international – pour la divulgation rapide de l'identité et l'adresse physique d'un abonné avec une adresse IP spécifique ou un compte utilisateur.**
- **Considérer la possibilité et le champ d'application d'une injonction de produire internationale qui doit être envoyée directement par les autorités d'une Partie aux agents des services répressifs d'une autre Partie.**
- **Considérer de renforcer la coopération directe entre autorités judiciaires pour ce qui concerne les demandes d'entraide.**

Résultats de l'évaluation ► Recommandations

- **Prendre en considération la pratique des services policières et judiciaires, d'obtenir des données spécifiées relatives au trafic et aux abonnés, directement auprès des fournisseurs de services étrangers, sous réserve de sauvegardes et de conditions.**
- **Considérer les enquêtes communes et/ou l'établissement d'équipes communes d'enquête entre les Parties.**

Suites à donner

Les Parties sont invitées à donner suite aux recommandations relevant de la responsabilité des autorités nationales et à rendre compte au T-CY dans les 18 mois suivant l'adoption du présent rapport sur les mesures prises, afin de permettre aux règles de procédure, d'examiner les progrès accomplis.