West African Cybersecurity and Cybercrime Workshop

Dakar, Senegal, 18-20 September 2012

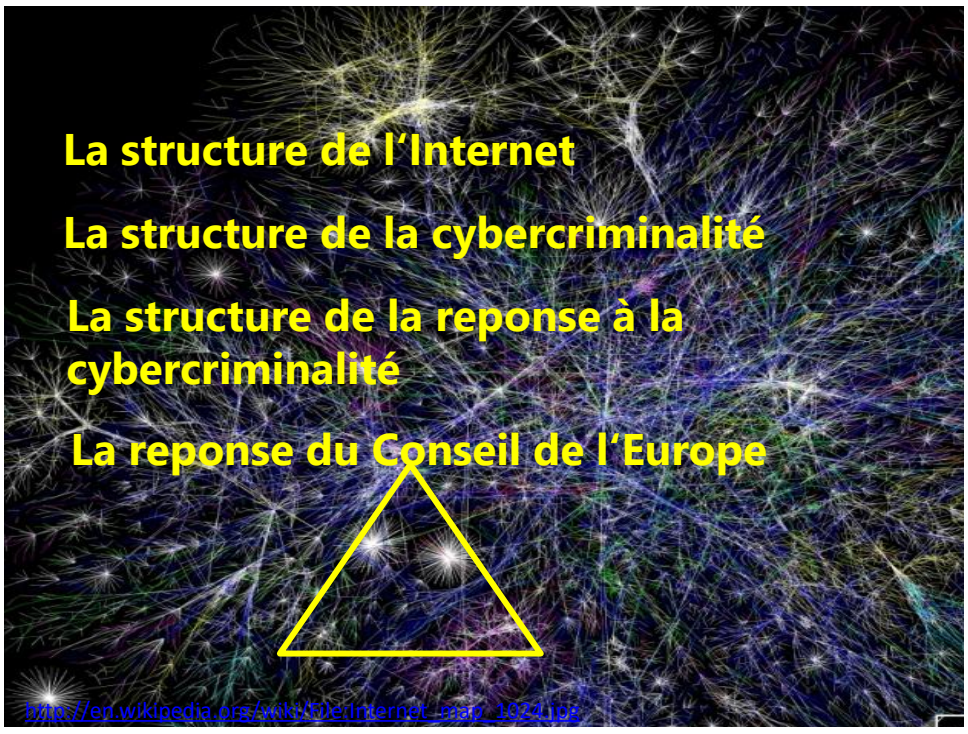
Stratégies contre la cybercriminalité – L'approche du Conseil de l'Europe

Alexander Seger

Council of Europe

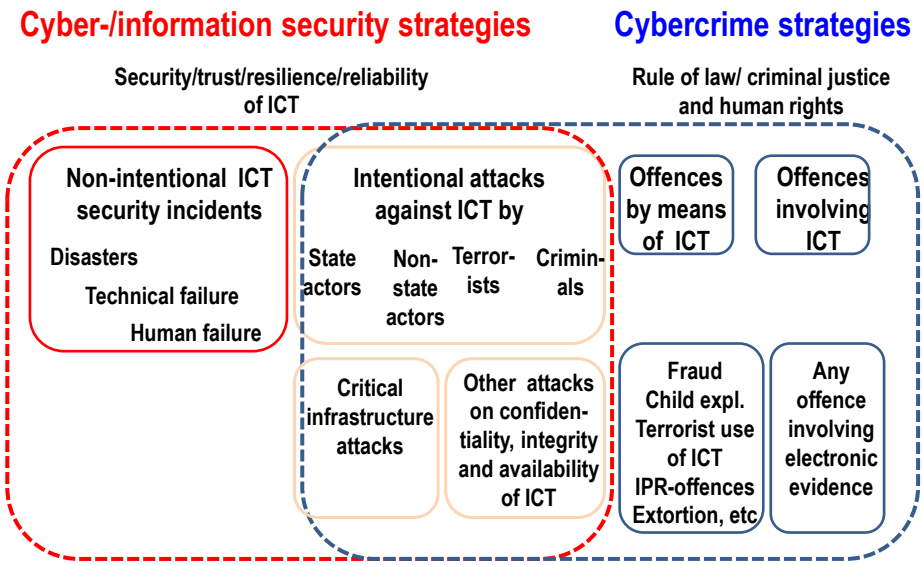
alexander.seger@coe.int www.coe.int/cybercrime

1



2

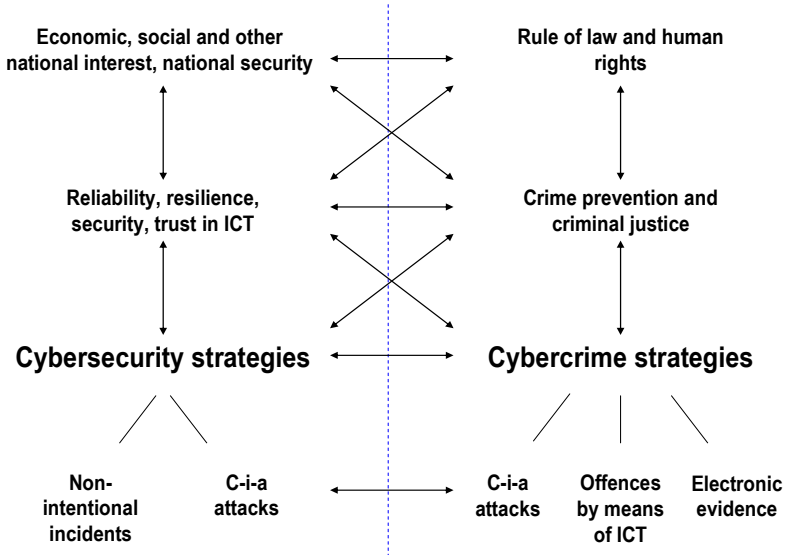
Cybercrime vs cybersecurity



3

3

Cybercrime AND cybersecurity



4

4

www.coe.int/cybercrime

4

Stratégies contre la cybercriminalité

Objectives:
assurer une reponse efficace de la justice pénale aux infractions contre et par le bias des données et système informatiques ainsi quant à toute infraction impliquant des éléments de preuve électroniques.

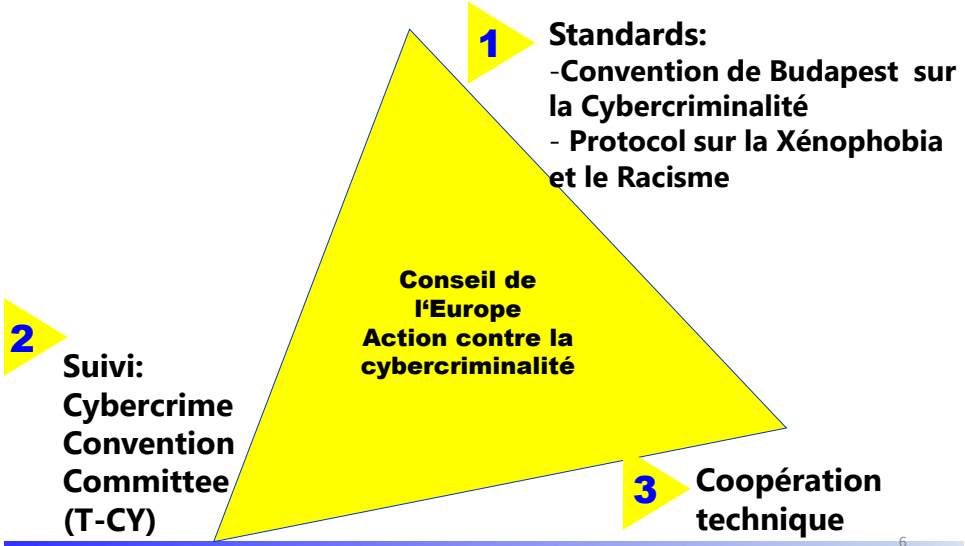
- Législation
- Mechanismes de reporting and analyse de la cybercriminalité
- Mesures préventives
- Unités d'enquête spécialisées (high-tech crime units)
- Coopération interservice
- Formation policière
- Formation judiciaire (juges, procureurs)
- Coopération publique/privée
- Coopération internationale efficace
- Investigations financières et prevention du fraude
- Protection des enfants

Discussion paper
„Cybercrime strategies“
www.coe.int/cybercrime
(Reports)

OU COMMENCER?

5

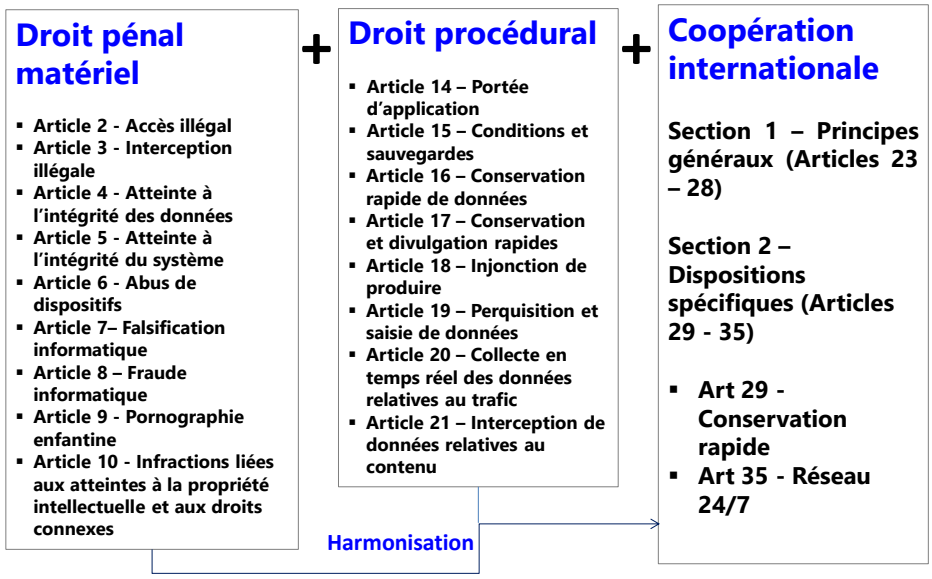
L‘approche du Conseil de l‘Europe contre la cybercriminalité



www.coe.int/cybercrime

6

1 Standards: La Convention de Budapest



Convention de Budapest: Processus d'adhésion

Article 37: La convention est ouverte à l'adhésion par les pays tiers

Processus d'adhésion:

1. **Préparer la legislation nationale**
2. **Une fois la législation adoptée ou à un état avancée, le gouvernement envoie un courrier au Secretaire Général du Conseil de l'Europe avec une demande pour lancer la consultation des parties à la Convention**
3. **Le secrétariat du Conseil de l'Europe effectuera les consultations et posera la question au Comité des Ministres**
4. **Après un vote positif le pays sera invité à accéder**
5. **Le pays est alors libre de décider quand accéder, à savoir déposer l'instrument d'accession**

Convention de Budapest: état actuel

- La Convention est entrée en vigueur en juillet 2004
- 37 ratification + 10 signatures (à la date du 1 septembre 2012)
- Signée par le Canada, le Japon, l'Afrique du Sud et ratifiée par les Etats-Unis et le Japon
- L'Argentine, l'Australie, le Chili, le Costa Rica, la Republique Dominicaine, le Mexique, les Philippines et le Sénégal ont été invités à adhérer
- Amendements législatifs en cours et adoptés dans de nombreux pays et accession à la Convention en considération

= La Convention fournit un cadre normatif global

La Convention de Budapest comme une loi modèle

- Utiliser comme "checklist"
- Comparer les articles

Voir profiles des pays sur

www.coe.int/cybercrime

Articles de la Convention	Disposition dans la legislation nationale
Art 4 Atteinte à l'intégrité du système	?
Art 6 Abus de dispositifs	?
Art 9 Pornographie infantine	?
Art 16 Conservation rapide	?

La Convention de Budapest comme une loi modèle

BC Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique.

Senegal Lois 2008-11 - Article 431-8

Quiconque aura accédé ou tenté d'accéder frauduleusement à tout ou partie d'un système informatique, sera puni d'un emprisonnement de six (6) mois à trois (3) ans et d'une amende de 1.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement

La Convention de Budapest comme une loi modèle

BC Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

Sénégal Lois 2008-11 - Article 431-13

Quiconque aura endommagé ou tenté d'endommager, effacé ou tenté d'effacer, détérioré ou tenté de détériorer, altéré ou tenté d'altérer, modifié ou tenté de modifier, frauduleusement des données informatisées, sera puni d'un emprisonnement d'un (1) an à cinq (5) ans et d'une amende de 5.000.000 à 10.000.000 francs ou de l'une de ces deux peines seulement.

2 Suivi: Concertation des Parties (Article 46)

Cybercrime Convention Committee (T-CY)

Toutes les parties au traité se concertent … afin de faciliter:

a l'usage et la mise en œuvre effectifs de la présente Convention …

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

3 Coopération technique

Fournir d'assistance: les projets contre la cybercriminalité

- **Projet Global contre la cybercriminalité (2006 – 2012)**
- **Projets joints de Union Européenne/Conseil de l'Europe dans plusieurs pays de l'Europe**

Eléments:

- **Devéloppement des stratégies sur la cybercriminalité**
- **Législation [analyses: Benin, Niger, Nigeria, Sénégal]**
- **Unités d'enquête spécialisées (high-tech crime units)**
- **Formation policière**
- **Formation judiciaire (juges, procureurs)**
- **Coopération publique/privée**
- **Coopération internationale efficace**
- **Investigations financières et prévention du fraude**
- **Protection des enfants**

Conclusion:
Coopération sur la base de la Convention de Budapest

Avantages

- **Coopération fiable et efficace entre les Parties**
- **Participation au Comité de la Convention sur la cybercriminalité (T-CY)**
- **Participation à l'établissement de normes futures (protocoles et autres compléments à apporter à la Convention de Budapest)**
- **Confiance accrue par le secteur privé**
- **Assistance technique et renforcement des capacités**

« Coût »: engagement à coopérer

Merci!

Inconvénients: ?

www.coe.int/cybercrime Alexander.seger@coe.int

15