COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Harmonisation du cadre légal sur la cybercriminalité en Afrique

Conditions pour l'action judiciaire contre la cybercriminalité

Rabat, 27-28 juillet 2010

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

Elements of the response to cybercrime

- LEA training
- Multi-stakeholder action (IGF, EuroDIG, Octopus)
- Judicial training
- Guideline for 100+ countries
- High-tech crime units
- **Budapest Convention**
  - Criminalising conduct
  - Investigative tools (procedural law)
  - Legal framework for international cooperation
- Protecting children
- LEA-ISP cooperation (guidelines 2008)
- Criminal money flows
- Public/private cooperation
- Efficient MLA
- CERT/CSIRTs, registries, registrars, ICANN
- 24/7 points of contact
- Prevention of terrorism
- Shared responsibility: Networks + initiatives
- Other treaties, laws and instruments
- Cloud computing?
- Human rights, data protection, rule of law principles

2

2

1 Legislation

Elaborer une législation compréhensive et harmonisée sur le plan international

- Criminaliser certaines conduites ▶ droit pénal matériel

- Donner aux forces de l'ordre/à la justice pénale les moyens d'enquêter, de poursuivre et de juger les cybercrimes (actions immédiates, preuve électronique) ▶ code de procédure pénale

- Permettre une coopération internationale efficace ▶ harmoniser la législation, faire des prévisions et établir des institutions pour la coopération policière et juridique, conclure ou prendre part à des accords

Legislation - Solution

La Convention sur la Cybercriminalité de Budapest

- Droit pénal matériel
- Droit procédural
- Coopération internationale

- Utiliser la Convention comme une loi modèle pour la préparation de législation

- Considérer l'adhésion à la Convention (article 36)

2 Formation & specialisation

Principaux problèmes:

- Tous les juges, les procureurs et les enquêteurs doivent être prêts à faire face à la cybercriminalité et à la preuve électronique et avoir au moins une compréhension de base de ces technologies et les problèmes liés
- Certains enquêteurs ont besoin de se spécialiser
- Formation systématique et durable non disponible

Formation & specialisation - Solution

- Concept 2Centre: centres d'excellence pour la formation des forces de l'ordre
- Pour les juges et les procureurs: concept de formation du Conseil de l'Europe developpé en 2009
  1. L'institutionnalisation de la formation initiale
  2. L'institutionnalisation de la formation continue
  3. Des formations/modules standardisés et reproductibles
  4. L'accès aux matériels de formation ou d'autoformation
  5. Les centres pilotes de formation élémentaire et avancée
  6. L'enrichissement des connaissances par le travail en réseau
  7. La coopération public-privé

3 Coopération international

La cybercriminalité est la criminalité transnationale - nécessité d'une action internationale urgente

Solutions:

- Appliquer le chapitre 3 de la Convention de Budapest + considérer l'adhésion
- Assurer une utilisation du canal d'Interpol, la coopération directe et et de réseau 24 /7
- Assurer une entraide judiciaire formelle plus efficace + combiner avec des mesures immédiates et urgentes

4 Sécurité ET droits fondamentaux

- Définir les pouvoirs de l'application de la loi par la loi
- Fournir des conditions et des garanties (article 15 de la Convention de Budapest)
- Adopter une législation sur la protection des données (utilisation du traité 108 du Conseil de l'Europe en tant que ligne directrice)

5 Coopération public-privé

Lignes directrices
pour la coopération entre les organes de répression et fournisseurs de services internet contre la cybercriminalité

Ont été adoptées pendant la Conférence « Coopération contre la cybercriminalité (Conseil de l'Europe, Strasbourg, France) des 1er-2 avril 2008 :

- **Lignes directrices communes**
- **Mesures à prendre par les forces de l'ordre**
- **Mesures à prendre par les fournisseurs de services/**

Lignes directrices

Common guidelines for LEA and ISP:

- Develop a culture of cooperation
- Develop written procedures for cooperation with each other
- Cooperate for the protection of rights and freedoms of individuals
- Respect each others roles, rights and limitations
- Mindful of cost of cooperation
- Etc

Coopération public-privé

Lignes directrices

Measures to be taken by law enforcement

- Broad and strategic cooperation with ISP
- Procedures for legally binding requests
- Designated and trained personnel for cooperation
- Verification of source of requests
- Standard request format
- Specificity and accuracy of requests
- Follow preservation orders with production/disclosure orders
- Criminal compliance programme
- International requests: 24/7 network and formal mutual legal assistance

Coopération public-privé

Lignes directrices

Measures to be taken by ISPs

- Report criminal incidents
- Assist LEA with training and other support
- Procedures for responding to requests
- Designated and trained personnel for cooperation
- Emergency assistance outside business hours
- Criminal compliance programme
- Verification of source of requests
- Standard response format
- Explanation for information not provided
- Coordination among ISP

Coopération public-privé

Lignes directrices

Important:

- Guidelines, not binding
- Not substitute for procedural law and other formal regulations
- Based on good practices already available
- Help LEA and ISP in any country to structure their cooperation
- Adaptable to specific situation and needs of each country

Coopération public-privé

Lignes directrices

Developments:

- Romanian government decision (Jan 09): judicial, law enforcement, regulatory bodies to make use of guidelines
- France: guidelines used for LEA-ISP agreement (Spring 2009)
- EU JAI Council conclusions (Nov 08): General support to CoE LEA-ISP guidelines + 8 specific ones
- Support implementation through Project on Cybercrime and other means (eg workshops in Ukraine and India in Spring 2009)
- Guidelines reflected in the judgment of the European Court of Human Rights K.U. v. Finland (application no. 2872/02)
- Memorandum of Understanding signed in Georgia (May 2010)
- Expand guidelines to other sectors (financial institutions)?

6 Conclusions

Construire une approche cohérente sur la cybercriminalité

- La législation sur la base de la Convention de Budapest
- Des unités spécialisées
- La formation sur l''application de la loi, les procureurs, les juges
- La coopération public-privé (y compris les ISP)
- La coopération internationale
- Les conditions et sauvegardes
- La législation de la protection des données

Fournir une assistance technique
par les donateurs / organisations internationales

Alexander.seger @ coe.int