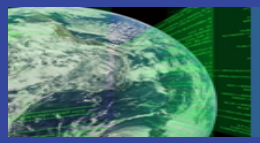


GLACY+
Global action on Cybercrime Extended
Action Globale sur la Cybercriminalité Elargie

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Convention de Budapest et perspectives

La Convention de Budapest sur la cybercriminalité et les perspectives du Conseil de l'Europe face aux défis de la coopération internationale à l'ère numérique

Abuja, 11-13 septembre 2017

Adel Jomni
Enseignant-chercheur, Université de Montpellier
Directeur diplôme: Cybercriminalité et Droit
Expert au Conseil de l'Europe

Intervenant: **ADEL JOMNI**

- Enseignant-chercheur, Faculté et Droit et Science politique, Université de Montpellier (France)
- Directeur du diplôme d'Université: Cybercriminalité, Droit et sécurité de l'information
- Expert international auprès du Conseil de l'Europe
- Membre de l'European Cybercrime Training and Education Group (ECTEG - Europol)
- Co-directeur de la session Ecole Nationale de la Magistrature (ENM- Paris) sur la Cybercriminalité et la preuve numérique
- Membre-fondateur du CECyF (Centre d'excellence français pour la lutte contre la cybercriminalité)

- **adel.jomni@umontpellier.fr**

Objectifs de la présentation

- Introduction générale sur les nouveaux défis liés au développement du numérique
- Introduction sur les objectifs et les idées qui ont présidé à l'élaboration de la Convention de Budapest sur la Cybercriminalité et la preuve électronique
- Présentation des principaux articles de la Convention

Société de l'information

- L'emprise des technologies numériques sur tous les secteurs d'activités humaines a favorisé l'avènement d'un nouveau type de société dénommée la société de l'information
- C'est une révolution, à l'image de la révolution industrielle au XVIII siècle
- Une nouvelle réalité qui se vérifie dans notre quotidien:
  - au travail,
  - à la maison
  - dans la majorité de nos loisirs

Innovations numériques et nouveaux modèles économiques

Le numérique est un formidable vecteur de transformation de l'économie mondiale par le caractère exponentiel de sa croissance et sa capacité à irriguer tous les secteurs de l'économie

- Le numérique s'impose comme un véritable moteur de croissance qui génèrera 64% de la croissance mondiale en 2017 pour atteindre 1674 milliards de dollars
- La contribution du numérique au PIB annuel de l'Afrique pourrait passer de 18 milliards de dollars à 300 milliards de dollars en 2025* (tous les pays n'abordent pas la vague numérique de la même façon)
- L'économie numérique européenne croît sept fois plus vite que tout autre secteur (2.000 milliards d'euros)

Sources: Credoc, INSEE, IDC, McKinsey

Numérique: liberté, dépendance et absence de frontières

- Les pays, les individus et les économies dépendent et se servent des réseaux et des technologies de l'information et de la communication
- Le nombre d'internautes fin 2016 est d'environ 3,9 milliards (environ 47 % de la population mondiale)
- Les informations et les connaissances peuvent être obtenues librement et démocratiquement
- L'information est ouverte, chacun peut y accéder
- Il n'y a plus de distance physique entre les gens, où qu'ils se trouvent

- Le cyberespace n'est pas concerné (ou presque) par les frontières politiques

Nouvelles formes de criminalité ou délinquance

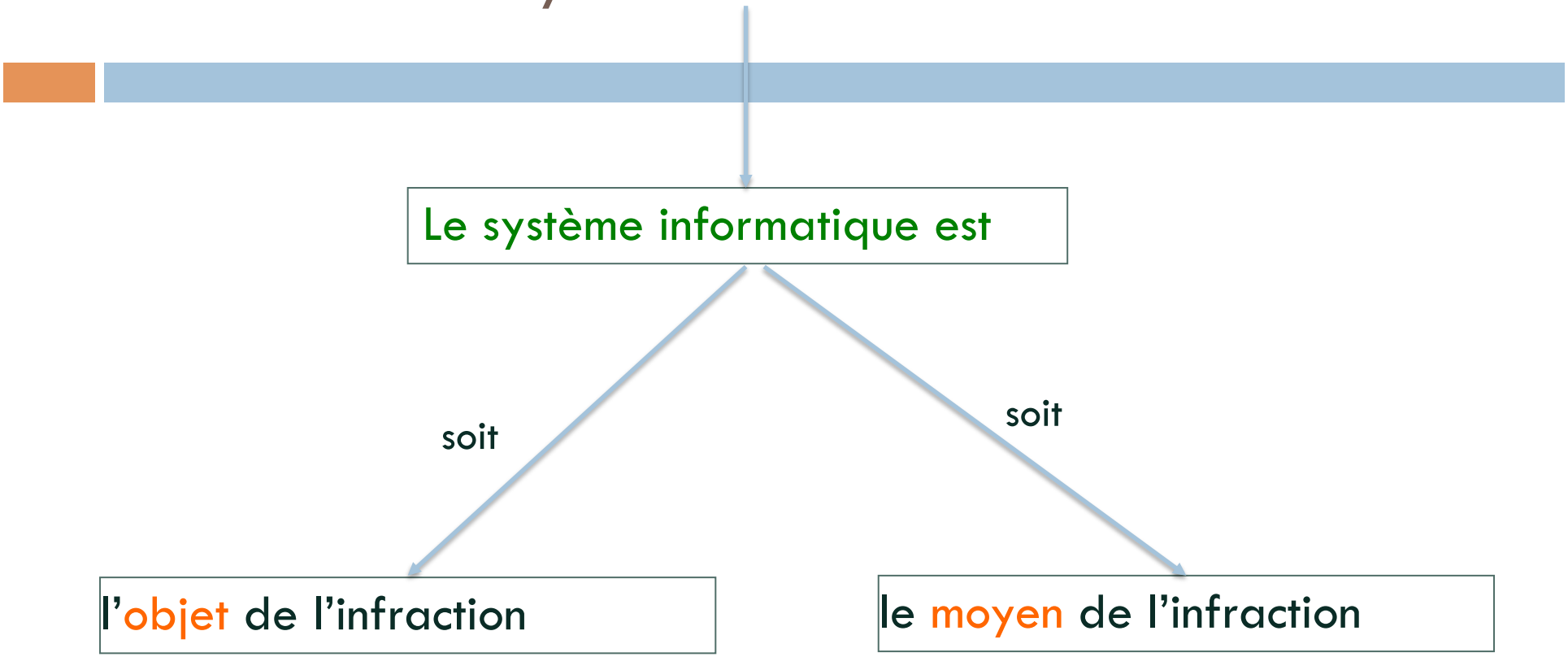
Toute invention humaine porteuse de progrès, peut être aussi génératrice de comportements illicites. … la société de l'information en général et les systèmes d'information en particulier n'échappent pas à cette règle.

Définition: Cybercriminalité

Selon la commission européenne, la cybercriminalité englobe trois catégories d'activités criminelles :

- Les infractions propres aux réseaux électroniques
- Les formes traditionnelles de criminalité (escroquerie, vols de données , fraudes, fausses cartes de paiement , usurpation d'identité en ligne)
- La diffusion de contenus illicites (pédopornographie, racisme)

Cybercriminalité



Système informatique

- Désigne (art 1 de la CdB) tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments, en exécution d'un programme, un traitement automatisé de données;

- C'est un système composé d'ordinateurs, de réseaux, de logiciels, de bases de données, … assurant la logistique du système d'information.

Données/information

- données informatiques (art 1 de CdB): désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;
- Données relatives aux trafics: désigne (Art 1 de la CdB) toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication indiquant l'origine, la destination, itinéraire, l'heure, la date, la taille, la durée de la communication ou le type de service sous-jacent

Quelques chiffres

- Les attaques par ransomware ont plus que doublé l'année dernière pour atteindre jusqu'à 4 000 attaques par jour.
- Le montant des rançons payées en 2016 a éte multiplié par 35 (de 24 millions de dollars à 850 millions de dollars).
- Les attaques par Ransomware se transforment également et sont de plus en plus automatisées du fait de la disponibilité et de l'accessibilité des services automatiques de logiciel malveillant comme les RaaS (ransomware as a service), la location de botnets et les services de harponnage.

La cybercriminalité profite des caractéristiques du Cyberespace

- Absence de barrières physiques et de frontières
- Liberté totale d'action sans contrainte territoriale
- Pas de limite géographique pour atteindre les victimes potentielles
- Anonymat
- Usage de fausses identités
- Absence de contact physique, dématérialisation

La diversité de l'activité cybercriminelle a été favorisée par l'interconnexion des réseaux et des systèmes d'information

Internet et Cybercriminalité

- Les Cybercriminels bénéficient de plus d'opportunités:
  - La preuve est volatile
  - Professionnalisation du Cybercrime CaaS
  - Inadéquation avec le principe traditionnel de la compétence territoriale des juridictions pénales et aux moyens d'enquête strictement encadrés par la loi
- La coopération internationale intervient entre pays ayant des cultures différentes, traditions juridiques différentes et un droit pénal différent

Cybercriminalité et prééminence du droit dans le cyberespace

- Cybercriminalité = ?
- Consignation par la police = 100
  - Enquêtes
  - Poursuites
- Jugements = 1 or 0.1 or 0.01?

Question: les gouvernements respectent-t-ils l'obligation qui leur est faite de préserver la société de la délinquance et de protéger les droits des victimes?

Quelles solutions?

- Pour garantir l'Etat de droit dans le cyberspace

- Pour réconcilier la nécessité d'un accès efficace aux données à des fins répressives et garantir le respect des exigences en matière de droits de l'homme et de l'Etat de droit

Quelques initiatives internationales dans la lutte contre la cybercriminalité

- Nations Unies
- Interpol
- Europol
- Union Européenne
- Conseil de l'Europe
- Union africaine
- CEDEAO

La Convention sur la Cybercriminalité du Conseil de l'Europe

connue sous le nom de la Convention de Budapest

- est le seul instrument international cohérent et rassembleur en matière de de lutte contre la cybercriminalité et de recueil de la preuve numérique
- est le premier traité international sur les infractions pénales commises via l'Internet
- permet une harmonisation des règles de procédure d'obtention de preuve en matière de coopération policière, d'entraide judiciaire et d'extradition
- Il est complété par le **Protocole relatif à l'incrimination d'actes de nature raciste et xénophobe** commis par le biais de systèmes informatiques.
- sert de lignes directrices pour tout pays élaborant une législation exhaustive en matière de cybercriminalité, mais aussi de cadre pour la coopération internationale contre la cybercriminalité parmi les Etats Parties.
- Compatible avec les conventions et les directives développées depuis quelques années (Malabo, directives CEDEAO, ..)

Résumé des objectifs de la CdB

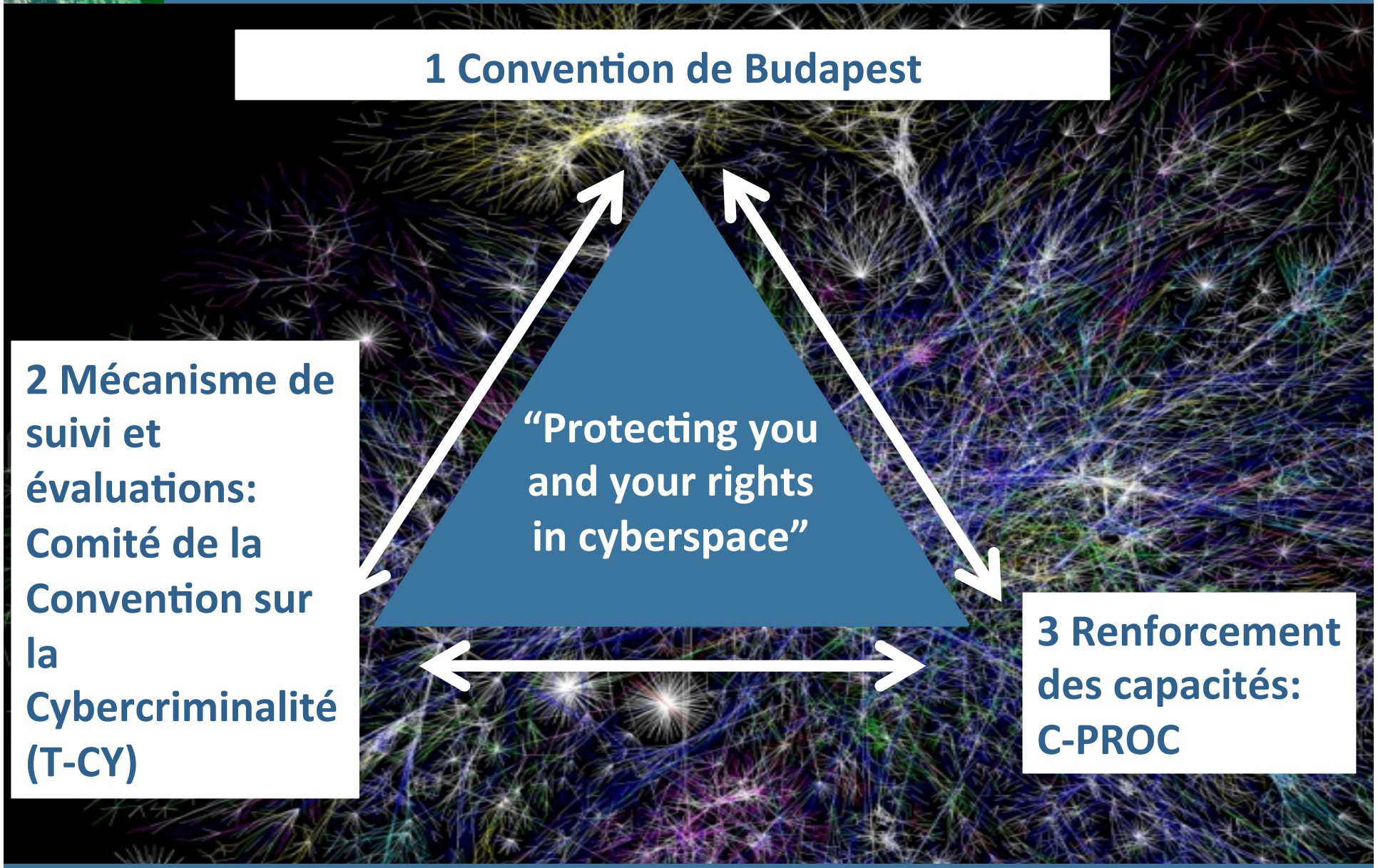
- poursuivre "une politique pénale" commune destinée à protéger la société contre le cybercrime, notamment par une harmonisation des:
  - comportements devant être réprimés dans les droits nationaux: l'adoption d'une législation appropriée
  - règles de procédure et des moyens d'obtention de preuve au niveau national
  - règles d'obtention de preuve en matière de coopération policière, d'entraide judiciaire et d'extradition: La maîtrise et l'usage des outils de coopération policière et judiciaire sont indispensables

Un Etat ne peut pas lutter seul contre ce phénomène criminel

Informations générales

- Début des travaux de réflexion :1997
- Adoption: Novembre 2001
- Budapest 23 novembre 2001:
  - Traité ouvert à la signature des Etats membres et des Etats non membres qui ont participé à son élaboration
  - et à l'adhésion des autres Etats non membres
- Situation au 9/9/2017: **Nombre total de ratifications/adhésions: 55 pays**
- Invités à adhérer: Maroc, Tunisie, Cap Vert et Burkina-Faso
- L'appropriation de la CdB dépasse largement les frontières de l'Europe: les USA, le Canada, le Japan, l'Australie, la République dominicaine, l'île Maurice, le Sri Lanka, Sénégal, Maroc, et les îles Tonga en font partie.
- plus de 70 pays supplémentaires ont pris la convention comme source d'inspiration pour élaborer leur législation interne.

Renforcement de l'Etat de droit dans le cyberspace: la Convention de Budapest sur la cybercriminalité



Comité de la Convention sur la cybercriminalité (T-CY)

Etabli d'après l'article 46 de la Convention de Budapest

Membres

(statut datant de juin 2016):

- 55 membres (Etats Parties)
- 12 Etats Observateurs
- 10 organisations internationales (African Union Commission, ENISA, European Union, Europol, INTERPOL, ITU, OAS, OECD, OSCE, UNODC)

Fonctions:

- Faciliter de l'usage et la mise en œuvre effective de la Convention, l'échange d'informa
- Evaluation de la mise en œuvre des dispositions de la Convention de Budapest par les Parties
- Notes d'orientation
- Rédaction de nouveaux instruments juridiques
- Etc.

Convention de Budapest: champs d'application

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Conduites pénalisées:

- Accès illégal
- Interception illégale
- Atteinte à l'intégrité des données
- Atteinte à l'intégrité du système
- Abus de dispositifs
- Fraude et falsification
- Pornographie enfantine
- Infractions PI

+

Outils procéduraux:

- Conservation rapide
- Injonction de produire
- Perquisition et saisie
- Interception de données informatiques

+

Coopération internationale:

- Extradition
- Entraide judiciaire
- Information spontanée
- Conservation rapide
- Entraide judicaire pour l'accès à des données informatiques
- Entraide judiciaire pour l'interception
- Points de contact 24/7

Harmonisation

Convention de Budapest: Champs d'application

- Mesures à prendre au niveau national:
  - Section 1: Droit pénal matériel (Art 2 …Art13)
  - Section 2: Droit procédural (Art 14 …Art21)
  - Section 3: Compétence (Art 22)
- Coopération internationale
  - Principes généraux (Art 23..Art 28)
  - Dispositions spécifiques (conservation et divulgation des données, entraide, ..) Art 29…35
- Clauses finales (Signature, Adhésion, ..) : Art 36..Art48

Merci de votre attention

Questions?