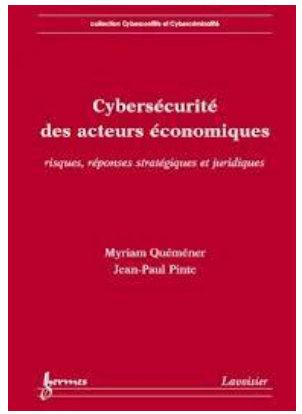
CLUSIF

Cybercriminalité et cybersécurité : réponses européennes et internationales

Myriam Quéméner

Magistrat, expert conseil de l'Europe



La Cybercriminalité, Délinquance Mondiale

- Délinquance se jouant des frontières
- Les cyberdélinquants repèrent les « cyberparadis » , pays à la législation faible ou inexistante.
- Volatilité des sites et hébergements dans ces pays
- Comment concilier la souveraineté des Etats et la lutte internationale contre ce phénomène?

Les Enjeux

- Nécessité de se mobiliser face à la hausse des cybermenaces
- Coordonner les actions
- enjeux géopolitiques , économiques , de santé publique

Le Programme Européen de Lutte contre la Cybercriminalité

- 12/02/2013 : Dans sa nouvelle stratégie, l'UE établit une approche commune en matière de sécurité des réseaux numériques, de lutte contre la criminalité en ligne et de protection des consommateurs.
- La criminalité en ligne est en forte croissance. Les virus informatiques, les infiltrations de réseaux et la **cybercriminalité**
- ec.europa.eu/news/science/130212_fr.htm

Directive 2013/40/UE du Parlement Européen et du Conseil

Relative aux attaques contre les systèmes d'information et remplaçant la décision-cadre 2005/222/JAI du Conseil du 12 août 2013

- Elle vise à harmoniser les législations en vigueur en matière de lutte contre la cybercriminalité et à instaurer une coopération renforcée dans l'Union européenne par la mise en place d'un système coordonné de suivi des infractions. Cette directive devra être transposée en droit interne d'ici le 4 septembre 2015

Règlement n° 611/2013 de la Commission Européenne du 24 juin 2013

- Concernant les mesures relatives à la notification des violations de données à caractère personnel en application de la directive 2002/58/CE sur la vie privée et les communications électroniques a été publié au Journal officiel de l'Union européenne du 26 juin 2013.
- Le règlement est entré en vigueur le 25 août 2013.

Notifications de Violation de Données Personnelles : une Nouvelle Téléprocédure

- Régulièrement, les médias se font l'écho de comptes clients dérobés lors d'attaques informatiques ou dévoilés sur internet en raison d'une mauvaise configuration du site web. De telles erreurs se multiplient,
- Publié le 24 juin 2013, le règlement européen relatif aux failles de sécurité (dit " data breach ") impose aux autorités de protection des données de mettre à disposition un moyen électronique sécurisé dédié aux notifications de violations de données personnelles. Pour répondre à cette exigence, la CNIL met en place une nouvelle téléprocédure sur son site Internet.

L'Enisa

- L'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA) vise à renforcer la capacité de l'Union européenne (UE), des pays de l'UE et du secteur des entreprises, en matière **de prévention, de réaction et de gestion des problèmes liés à la sécurité des réseaux et de l'information**.
- L'ENISA prête **assistance** et fournit des **conseils** à la Commission et aux pays de l'UE. L'agence peut également être appelée à **aider la Commission à mener les travaux techniques préparatoires** pour la mise à jour et le développement de la législation de l'UE.
- En outre, l'ENISA doit **faciliter et encourager la coopération** entre les acteurs des secteurs public et privé et, ainsi, permettre de parvenir à un niveau de sécurité suffisamment élevé dans les pays de l'UE.
- www.**enisa**.europa.eu

Rôle d'Interpol

- Le programme de lutte contre la cybercriminalité d'INTERPOL s'articule autour de la formation et des opérations, et s'emploie à suivre l'évolution des menaces. Il vise à :
- développer l'échange d'informations entre pays membres par l'organisation de ☐ groupes de travail régionaux et de conférences ;
- dispenser des ☐formations afin de faire acquérir aux participants un certain niveau professionnel et de leur permettre de le maintenir ;coordonner et appuyer des opérations internationales ;dresser une liste mondiale d'officiers de contact joignables 24 heures sur 24 pour les besoins des enquêtes relatives à des affaires de cybercriminalité ;apporter une assistance aux pays membres en cas de cyberattaque ou dans le cadre d'enquêtes sur des affaires de cybercriminalité, en mettant à leur disposition des services en matière de recherche et de bases de données ;
- établir des partenariats stratégiques avec d'autres organisations internationales et avec des organismes du secteur privé ;détecter les nouvelles menaces et communiquer aux pays membres les renseignements recueillis ;mettre à disposition un portail Web sécurisé permettant d'accéder à des informations et à des documents présentant un intérêt opérationnel.

Eurojust

- Eurojust est confronté à une amplification remarquable de ses interventions, ce qui signale l'importance croissante de la coopération judiciaire pénale dans l'UE. D'abord quelques données statistiques. Avec 1533 cas transmis en 2012, Eurojust a enregistré une hausse des dossiers traités de l'ordre de 6% par rapport à l'année précédente. Pas moins de 194 réunions de coordination ont porté notamment sur le trafic d'êtres humains et de drogue et sur les fraudes. L'aide à l'exécution du Mandat d'Arrêt Européen, quant à elle, a concerné quelques 250 cas.
- L'augmentation des dossiers s'accompagne d'ailleurs d'une diversification des défis détectés, qui ont à faire notamment avec la piraterie maritime et la cybercriminalité.

Le Centre Européen de Lutte contre la Cybercriminalité (EC3) sera Inauguré le 11 janvier 2013

- Le Centre européen de lutte contre la cybercriminalité (EC3) contribue à protéger les entreprises et les citoyens européens contre la cybercriminalité.
- «*Le centre de lutte contre la cybercriminalité va accroitre la capacité de l'UE à combattre la cybercriminalité et à défendre un internet libre, ouvert et sûr.*

Missions de EC3

- Conformément à la Convention de Budapest sur la cybercriminalité, le champ d'application de EC3 englobe les crimes qui sont dirigés contre les infrastructures informatiques et de réseau, ainsi que les crimes commis en ligne. Elle couvre tous les crimes contre les programmes malveillants, piratage, phishing, intrusions, la manipulation, le vol d'identité et la fraude, à la toilette et l'exploitation sexuelle des enfants en ligne.
- Point focal (FP) Cyborg soutient les États membres de l'UE dans la prévention et la lutte contre les différentes formes de cybercriminalité, en particulier ceux liés à la cybercriminalité groupes ou organisations criminelles.

Fraude par Cartes de Paiement

- Risque faible et l'activité criminelle très rentable qui apporte les groupes du crime organisé (GCO) de provenance de l'UE un revenu annuel d'environ 1,5 milliards d'euros.
- Terminal Point Focal fournit un soutien aux autorités répressives de l'UE (LEA) à des centaines d'enquêtes internationales PCF ..L'équipe spécialisée de produire des rapports d'analyse et facilite la coopération pour lutter contre les crimes PCF. Un soutien est apporté sur place par le bureau mobile, qui permet l'accès aux bases de données d'Europol via une connexion sécurisée. En outre, un kit de dispositif d'extraction médico-légale universel (UFED) peut être déployé, qui est capable d'obtenir des données à partir de périphériques de stockage de données numériques, par exemple les téléphones, les PDA, les appareils de navigation et les cartes SIM. Un lecteur de carte permet une vérification rapide des données sur une carte de paiement et une base de données avec des numéros de carte peut donner des informations sur l'émetteur de la carte.

Lutte contre l'Exploitation Sexuelle

- Exploitation sexuelle des enfants »fait référence à l'agression sexuelle d'un être humain âgé de moins de 18 ans. Il comprend la production d'images d'abus d'enfants et leur diffusion en ligne comme des formes particulièrement graves de criminalité commis contre des enfants.
- PF Twins vise à identifier les auteurs et d'établir des liaisons transversales au sein des États membres participants. Il identifie en outre modus operandi transfrontalier et analyse les méthodes de communication des réseaux criminels, en vue de démanteler ces réseaux.
- Le FP met également l'accent sur l'identification des victimes, en vue d'arrêter éventuellement en cours d'exploitation et de permettre d'engager des mesures de soins par les autorités compétentes. FP Twins coopère sur le plan opérationnel par les officiers de liaison Europol »(ELO) réseau, fournit un soutien analytique stratégique et opérationnelle, et soutient des projets internationaux tels que COSPOL Internet associé à l'enfance d'abus projet Matériel (CIRCAMP) et la Coalition européenne financier (CEF).

La Protection Face à l'Espionnage Numérique

- Les entreprises innovantes sont de plus en plus exposées à des pratiques malhonnêtes, trouvant leur origine dans l'Union ou ailleurs, qui visent l'appropriation illicite de secrets d'affaires, notamment le vol, la copie non autorisée, l'espionnage économique ou le non-respect d'exigences de confidentialité. Les évolutions récentes (mondialisation, recours croissant à la sous-traitance, allongement des chaînes D'approvisionnement ou usage accru des technologies de l'information et des communications) contribuent à la hausse de tels risques.

Vers la Protection du Secret des Affaires

- En Europe, 25% des entreprises se sont plaintes de vol d'informations confidentielles en 2013, selon un sondage cité par la Commission.
- **La Commission européenne a proposé le 5 décembre 2013 un projet de directive visant à protéger les secrets d'affaires, souvent des technologies ou savoir-faire particuliers, contre le vol par des entreprises concurrentes.**
- Le projet de directive prévoit des dommages et intérêts pour les entreprises victimes d'un vol ou d'une appropriation illicite de ces informations confidentielles.

http://ec.europa.eu/internal_market/iprenforcement/docs/trade-secrets/131128_proposal_fr.pdf

Conseil de l'Europe

- La Convention de Budapest sur la cybercriminalité, entrée en vigueur en juillet 2004
- Seul traité international contraignant
- Sert de ligne directrice à tout Etat souhaitant développer une législation nationale complète contre la cybercriminalité
- Propose un cadre pour l'élaboration d'une législation et la mise en place d'une coopération internationale
- Site : http://www.coe.int

Les Grands Axes de la Convention

- Droit pénal matériel : impose de qualifier en infractions les atteintes à l'intégrité des systèmes, la fraude informatique…
- Droit procédural : engager des poursuites, moyens d'investigation et sanctions
- Coopération internationale : point de contact 24/24

Terminologie et définitions

- Système informatique: tout dispositif isolé ou ensemble de dispositifs interconnectés assurant un traitement automatisé de données
- Données informatiques: toute représentation de faits , d'informations ou de concepts spus une forme qui se prête à un traitement informatique , y compris un programme de nature en sorte qu'1 système exécute une fonction

Définition des Fournisseurs de Services

- Entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique , et toute entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs

Les Données Relatives au Trafic

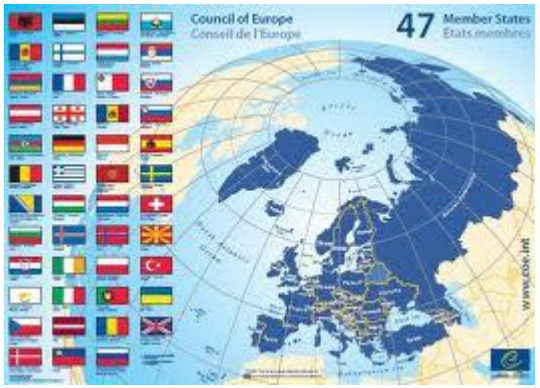
- Toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication
- Origine , destination , itinéraire, heure, date, taille, durée de la communication ou type de service sous-jacent.

Les Infractions contre la Confidentialité, l'Intégrité et la Confidentialité

- Accès illégal (article2)
- Interception illégale (article3)
- Atteinte à l'intégrité des données (article4)
- Atteinte à l'intégrité du système (article5)
- Abus de dispositif(article6)

Les Infractions Informatiques

- Falsification informatique(art.7)
- Fraude informatique (art.8)



Les Infractions se Rapportant au Contenu

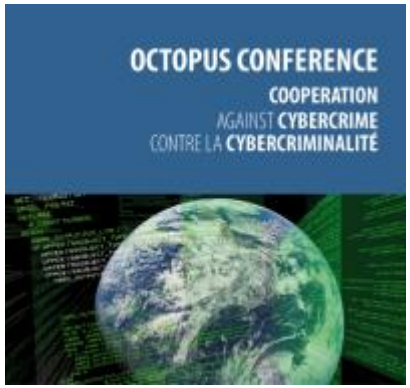
- Infractions se rapportant à la pornographie enfantine (art.9)
- Production
- Offre ou mise à disposition
- Diffusion et transmission
- Le fait de se procurer de la pornographie enfantine par le biais d'un système informatique
- La possession de pornographie enfantine dans un système informatique

Moyens d'Investigation

- La Convention prévoit des règles de base pour la conduite d'enquêtes dans le monde virtuel et qui représentent de nouvelles formes d'entraide judiciaire.
- Ainsi sont prévues : la conservation des données stockées la conservation et divulgation rapide des données relatives au trafic, la perquisition des systèmes et la saisie de données informatiques, la collecte en temps réel des données relatives au trafic et l'interception de données relatives au contenu.

Etat des Signatures

- Nombre total de signatures non suivies de ratifications : 11
- Nombre total de ratifications/adhésions : 41



Perspectives

- Au delà des textes , élaborer une véritable politique pénale en matière de lutte contre la cybercriminalité
- Création d'un maillage par le biais des centres européens en matière de cybercriminalité
- Coopération public / privé et renforcement de la coopération internationale
- Codification , lisibilité , interministérialité

- Merci de votre attention
- myriam.quemener@hotmail.fr