

Mercredi 1 Avril 2020

Synthèse de documents : la fraude sur internet

Corpus

Document 1, « Les fraudes sur internet se multiplient », Le Figaro, 2010.

Document 2, « Pas encore la cyberguerre, quoique ? », Steven Coissard et Clémentine Hottier.

Document 3, « L'irrésistible appel du hacking », Joseph Menn, Financial Times, 2 novembre 2011.

Document 4, Juan Osborne, *Anonymous*.

Consignes

Première partie (synthèse) : Vous ferez une synthèse concise, objective et ordonnée en confrontant les documents du corpus. (40 pts)

Deuxième partie (écriture personnelle) : Selon vous, le hacking, à des fins politiques, est-il défendable ? (20 pts)

Document 1 : Les fraudes sur internet se multiplient

Combattre les fraudes à la consommation sur internet est une tâche ardue, alors que la coopération transfrontalière et entre les différents interlocuteurs reste balbutiante et que les régulateurs sont à la traîne des cybercriminels, selon les acteurs de la lutte eux-mêmes.

"Profitant des lacunes de l'espace judiciaire européen, qui devient un véritable « no man's land » dans un contexte transfrontalier, la fraude s'exerce en tout lieu et a un champ d'action mondial", s'alarme la directrice générale d'Euro-Info-Consommateurs Martine Mérieau. Cette association franco-allemande basée à Kehl, sur la rive droite du Rhin, organisait jeudi à Strasbourg un colloque sur le thème "Criminalité sur internet, le consommateur est-il bien protégé en Europe ?".

Les fraudes commises contre les consommateurs en Europe se "multiplient", souligne Mme Mérieau. Selon l'étude "The European Marketplace: Consumer Complaints 2008-2009", le réseau des Centres européens de consommateurs, présents dans les 27 Etats membres de l'Union

européenne, en Islande et en Norvège, a enregistré en 2007 2.583 plaintes concernant le e-commerce, 3.356 en 2008 (+30%) et 4.921 en 2009 (+47%).

Cette augmentation se nourrit de plusieurs facteurs: la croissance des échanges sur internet, leur caractère transfrontalier quand la régulation de la Toile ne l'est guère et le manque de coopération entre acteurs privés et publics. "On a affaire à un système dont la plupart des opérateurs, des centres nerveux à la distribution aux consommateurs, sont des acteurs privés. (...) Il est parfois tentant pour les opérateurs de ne pas divulguer l'ensemble des informations, des difficultés sur le réseau", explique Hervé Dupuy, membre du cabinet de la commissaire européenne pour la Stratégie numérique Nelly Kroes.

Le sentiment d'insécurité nuit à l'envol des échanges transfrontaliers: seuls 8% des Européens interrogés lors d'une enquête "Eurobaromètre" de mars 2010 avait effectué lors des 12 derniers mois un achat en ligne auprès d'un autre pays de l'UE. Non que l'Union européenne soit restée inactive: la Commission a présenté en octobre 2008 une proposition de directive renforçant les droits des consommateurs et prenant en compte les nouvelles problématiques liées au "e-commerce".

Une plateforme de recueil des informations relatives à la cybercriminalité a été créée, hébergée par l'agence de coopération policière Europol, et est en train de "développer ses capacités", affirme Carlo van Heuckelom, chef du bureau criminalité financière de l'organisme.

Le Figaro, le 27 novembre 2010.

Document 2 : Pas encore la cyberguerre, quoique ?

La révolution des télécommunications, de l'information et des communications se traduit désormais en valeur marchande. La dernière étude menée par McKinsey montre qu'Internet représente en France 3,2% de croissance du PIB (60 milliards d'Euros) et plus d'un million d'emplois (2009).

Jamais Sun Tsu, général et stratège chinois du VI^e siècle avant J-C. qui décrivait l'information comme le nerf de la guerre, n'avait été autant d'actualité. A l'origine de création de richesses (25 milliards d'Euros de chiffre d'affaires pour le e-commerce en 2009), l'information fait l'objet de plus en plus convoitises, souvent illégales : le rapport de Symantec mentionne plus de 286 millions de programmes malveillants en 2010. Les formes d'attaques se développent : phishing (hameçonnage), pourriel, déni de service, défiguration de sites web, cybersquattage, hoax, virus, ver, cheval de Troie, botnet, bombe logique, scareware, espionnage... (pour plus d'informations, voir le 4^e forum international sur la cybercriminalité, 2010).

Les pirates du XXI^e siècle ne sont plus les hackers ou white-hat d'autrefois. Ces passionnés d'informatique dont l'objectif était d'explorer les limites des systèmes informatiques ou logiciels pour révéler, améliorer et résoudre leurs failles. Aujourd'hui, nous faisons face à des black-hats, des cybercriminels qui cherchent à nuire, à détruire et surtout à profiter frauduleusement de la création de valeurs issue des NTIC. La cybercriminalité, soit l'ensemble des infractions pénales commises via les réseaux de communications électroniques et les systèmes d'information ou contre ces derniers, est désormais une menace prise très au sérieux par les autorités publiques. Les Etats, et notamment la France, se dotent de moyens législatifs pour lutter contre ces nouvelles menaces (LOPPSI II), tentent d'anticiper les évolutions (Plan de développement de l'économie numérique 2012), renforcent leurs organismes de lutte contre la cybercriminalité (ANSSI, OCLCTIC)...

Ces actions menées par les Etats seront-elles suffisantes ou auront-ils toujours un temps de retard sur les pirates comme c'est déjà le cas avec HADOPI ? Ce qui est certain, c'est que rien ne sera possible sans une prise de conscience du grand public et des entreprises. Il est important de sensibiliser tous les acteurs de la vie économique. En France, les CCI et les gendarmeries proposent ce genre de formations gratuitement.

Pour autant, il ne faut pas tomber dans une paranoïa exagérée. La recrudescence de la concurrence, induite par la mondialisation de l'économie, conduit souvent à une disproportion dans l'utilisation de certains termes. Ainsi, il n'est pas rare de parler de guerre économique ou de cyberguerre.

Cependant, en droit international, le terme de guerre est restreint à une opposition entre deux Etats. Hors, en ce qui concerne la cybercriminalité, dans la très grande majorité des cas, les Etats ne sont pas mis en cause directement. Même en 2007, lorsque les systèmes d'information des institutions publiques et bancaires estoniennes ont été la cible d'attaques, aucune preuve n'a permis d'incriminer directement un autre Etat.

Steven Coissard et Clémentine Hottier, école supérieure de commerce, IDRAC, Lyon

Document 3 : L'irrésistible appel du hacking

Pratiqué par des groupes comme Anonymous et LulzSec, le sit-in virtuel, qui consiste à bloquer un site en l'attaquant, séduit de plus en plus.

L'irruption de la police à son domicile aux Pays-Bas n'a pas suffi à ébranler la foi de Martjin Gonlag, 19 ans, en Anonymous, le cybercollectif polymorphe qui terrorise les gouvernements et les grandes multinationales sur cinq continents. Interrogé pendant deux jours en 2010 avant d'être relâché dans l'attente d'un jugement qui pourrait le condamner à six ans de prison, le jeune homme n'en a pas moins décidé de télécharger un logiciel pirate pour participer aux attaques informatiques menées contre les sociétés Visa, MasterCard et autres ayant suspendu

tous les transferts d'argent au bénéfice de WikiLeaks, qui venait de publier les câbles de la diplomatie américaine.

Il existe tellement de failles de sécurité dans les systèmes informatiques que les services de renseignements considèrent les hackers comme l'une des principales menaces pour les pays occidentaux. S'ils redoutent avant tout les attaques orchestrées par des Etats, la frontière entre militants, criminels et espions devient de plus en plus floue. Gonlag, par exemple, fait partie de ces milliers de militants d'un nouveau genre qui soutiennent le mouvement dit "hacktivisme", mot formé à partir de *hacking* [piratage] et d'*activism* [militantisme]. Le plus connu des groupes de cette mouvance est Anonymous, un collectif virtuel permettant à des internautes relativement peu aguerris de participer à des mouvements de contestation souvent illégaux.

Pour ses partisans, le mouvement des hacktivistes reflète la place croissante de la technologie dans notre quotidien. Internet démocratise à la fois l'expression politique légitime et les opérations de piratage, de la même manière qu'il a démocratisé les médias en permettant à chacun de tenir un blog ou de publier un livre électronique. Pour ses opposants, parmi lesquels figurent les sociétés victimes de fuites sur Internet ou de vols de fichiers clients par des hacktivistes, Anonymous crée un dangereux précédent. Même du côté des sympathisants, certains craignent que l'entêtement du collectif ne provoque un retour de bâton législatif qui pourrait aboutir à un renforcement de la surveillance sur le réseau au détriment de la vie privée, si chère à Anonymous.

En théorie, la divulgation de ces informations privées avait pour but de faire l'actualité et de gêner les sociétés visées afin de les obliger à améliorer leurs systèmes de protection. Il s'agissait également de révéler la complicité de certaines sociétés de sécurité avec les autorités en matière de surveillance et de répression.

Toutefois, bon nombre d'Anonymous qui avaient soutenu les attaques de déni de service n'ont pas approuvé ces opérations antisécurité. D'autres ont manqué s'étouffer après la divulgation délibérée d'informations bancaires et de mots de passe de citoyens ordinaires. Certains membres se sont mis à penser que leurs chefs ne cherchaient qu'à accroître leur influence et étaient effectivement de mèche avec les réseaux du crime organisé, qui auraient pu exploiter les informations bancaires récupérées chez Sony après la neutralisation par Anonymous du système de sécurité.

Joseph Menn, Financial Times, 2 novembre 2011

Document 4 : Juan Osborne, Anonymous.

