الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ م إ

LETTRE D'INFORMATION DES ACTUALITES INTERNATIONALES
DANS LE DOMAINE DE LA LUTTE CONTRE LE BLANCHIMENT D'ARGENT ET LE FINANCEMENT DU TERRORISME

Lutte contre le cyber-jihadisme : Une course sans fin

Suspendre des milliers de comptes pour apologie ou promotion du terrorisme, comme vient de le faire Twitter, est une mesure nécessaire mais loin d'être suffisante pour entraver les actions des cyber-jihadistes, estiment des experts.

D'une part il reste facile de rouvrir, au fur et à mesure qu'ils sont fermés, de nouveaux comptes et d'autre part cette politique risque de pousser encore davantage les utilisateurs vers des réseaux sociaux plus confidentiels, cryptés ou protégés, voire vers le "web profond" ("darkweb" ou "deepweb"), partie obscure de l'internet non référencée dans les moteurs de recherche classiques.

"Suspendre plus de 235.000 comptes, comme vient de l'annoncer Twitter, peut avoir une influence, mais à très court terme" assure à l'AFP Gérôme Billois, expert au sein du Club de la sécurité de l'information français (Clusif). "Il y a des techniques bien connues par les jihadistes et les cybercriminels au sens large, qui sont de dire : mon compte Twitter s'appelait A, maintenant il s'appelle A1, A2, A3, etc… Ouvrir un compte, cela prend moins d'une minute. Ça peut même être partiellement automatisé".

"J'ai bien peur que le besoin, les envies de propagande ne soient plus forts que les actions que pourraient mener Twitter en coupant un certain nombre de comptes", ajoute-t-il.

Au cours des derniers mois de grands acteurs américains de l'internet, comme Twitter, Youtube ou Facebook ont été soumis à des pressions croissantes de la part des gouvernements, américain et autres, pour les amener à lutter davantage contre la propagande jihadiste en ligne et l'utilisation de leurs services par des réseaux jihadistes.

Ils assurent tous le faire et y consacrer de plus en plus de ressources, mais "la nature même d'internet fait que c'est une course sans fin, dans laquelle on est toujours un cran derrière", estime Gérôme Billois.

- 300 millions d'utilisateurs

Si Twitter ou d'autres réseaux sociaux grand public deviennent trop vigilants, les cyber-jihadistes seront incités à utiliser davantage des logiciels ou des applications plus difficiles à contrôler, comme par exemple Telegram, créé dans un but de confidentialité par deux Russes, dans lequel les échanges peuvent être cryptés.

Les services de renseignements préfèrent souvent laisser des forums ouverts, qu'ils peuvent surveiller, en activité plutôt que de voir leurs cibles migrer vers le darkweb ou la cryptographie.

"Il faut toujours penser stratégie, bataille, tactique militaire" explique à l'AFP le rhétoricien et philosophe Philippe-Joseph Salazar, auteur de l'essai "Paroles armées - Comprendre et combattre la propagande terroriste" (Lemieux éditeur). "Twitter était un terrain d'affrontement. Si ce terrain disparaît ou est moins facile, on déplace les bataillons ailleurs, c'est tout. Et là on se retrouve avec le problème de Telegram, ou du Darknet".
Pour l'expert américain Andrew Macpherson, spécialiste en cyber-sécurité au sein de l'University of New Hampshire, "il faut mesurer l'ampleur de la tache qui consiste à contrôler l'emploi des réseaux sociaux quand il y a plus de trois cents millions d'utilisateurs".
"Il est certain que les groupes terroristes continueront par tous les moyens d'utiliser les nouvelles technologies pour leur propagande", ajoute-t-il. "Comme ils chercheront toujours des moyens de maintenir et d'améliorer la confidentialité de leurs communications".
Pour cela, des logiciels d'anonymisation, de cryptage et de cyber-dissimulation sont faciles à trouver sur le web. Aucune compétence technique particulière n'est requise pour les utiliser, comme l'ont prouvé des affaires récentes dans lesquelles les enquêteurs ont été arrêtés dans leurs investigations par des téléphones cryptés, des messageries protégées par des mots de passe incassables ou des forums privés dans lesquels ils ne sont pas parvenus à pénétrer.
Et si les dispositifs de contrôle devenaient trop efficaces, le groupe Etat islamique, par exemple, dispose des compétences requises pour élaborer ses propres logiciels, assure Gérôme Billois.
"Vous mettez une équipe de quatre-cinq personnes avec les bonnes compétences et les bonnes motivations, ils vous lancent des services innovants qui peuvent être utilisés par des milliers de personnes", dit-il. "Et ces compétences, s'ils ne les ont pas entièrement, ils sont tout à fait capables de les acheter".
Lien : http://www.ladepeche.fr/article/2016/08/23/2405298-lutte-contre-le-cyber-jihadisme-une-course-sans-fin.html

La guerre financière contre Daech... éléments de réflexion

La guerre économique contre l'EI. *Voici le texte d'une dépêche de l'agence Reuters publiée le 25 novembre dernier. Elle décrit les nouveaux outils de la guerre économique actuellement menée par la coalition internationale contre les approvisionnements de Daech. En bombardant les camions citernes, mais aussi en s'appuyant sur les études menées par les services de renseignement pour traquer les « financiers » de l'organisation Etat islamique qui, selon un agent du FBI qui participait à une conférence à Washington il y a deux semaines, utilisent parfois « le circuit bancaire traditionnel ». Dépêche rédigée par Yeganeh Torbati et Brett Wolf*
Les bombardements des infrastructures pétrolières de l'Etat islamique en Syrie entamés par l'US Air Force le mois dernier dans le cadre de la guerre économique contre l'organisation fondamentaliste sunnite ont fait perdre à celle-ci un tiers de ses gains tirés de l'or noir, estiment les Etats-Unis.
Pour trouver leurs cibles, les avions américains se sont en partie appuyés sur une source non conventionnelle de renseignement : les données bancaires qui fournissent des informations pour déterminer les raffineries et les stations-service qui génèrent des liquidités pour le groupe. Le but est de couper l'EI de ses sources de financement

en mettant au jour les liens qu'il a encore avec le système financier international. En identifiant les flux financiers en provenance de l'EI et vers l'EI, les autorité américaines ont pu se faire une idée de la façon dont marche son économie souterraine, explique-t-on au sein des équipes au fait de ce travail. Et cela a à son tour eu une influence sur les cibles à viser par les frappes aériennes.

Cette tactique a été mise en place avant les attentats du 13 novembre à Paris et s'est intensifiée depuis, explique-t-on. *"Nous avons fait du vrai bon boulot en maintenant largement l'Etat islamique hors du système financier officiel*", estime Matthew Levitt, qui était chargé du renseignement au Trésor américain sous le gouvernement de George W. Bush. "*Mais le succès n'a pas été total et c'est peut-être pas une mauvaise chose*."

Reuters n'a pu vérifier quand cette campagne "Tidal Wave II" ("Raz-de-marée II") a exactement commencé ni quels sites ont été détruits en conséquence, ni même comment des documents bancaires ont pu être utilisés pour identifier les objectifs pétroliers de l'EI les plus lucratifs en Syrie.

Couper du systéme

Selon un rapport du Groupe d'action financière (Gafi), un organisme intergouvernemental de lutte contre le blanchiment d'argent et le financement du terrorisme, plus de 20 établissements financiers syriens sont présents dans les territoires contrôlés par l'EI en Syrie. En Irak, le Trésor américain travaille avec le gouvernement pour couper du système financier irakien et international les succursales bancaires se trouvant sur le territoire de l'EI.

Gerald Roberts, chef de section des opérations de financement du terrorisme au FBI, explique que les recrues de l'EI arrivent souvent en Syrie avec des traces financières ***"exploitables". "Nous les voyons utiliser le système bancaire traditionnel"***, a-t-il déclaré lors d'une conférence bancaire il y a dix jours à Washington. Les jeunes membres de l'EI pointus en matière technologique sont également habitués aux devises virtuelles telles le bitcoin, a-t-il ajouté.

Selon Matthew Levitt, l'EI est parfois contraint d'utiliser les banques commerciales quand les montants impliqués sont trop importants à déplacer par d'autres canaux.

Le réseau FinCEN du Trésor américain utilise une série de techniques pour repérer, dans les quelque 55.000 rapports reçus chaque jour des établissements financiers, les signes d'activité de l'EI, indique un porte-parole. Il n'a pas voulu décrire ces techniques, mais, expliquent des sources judiciaires et policières, les noms, les adresses IP, les adresses mails et les numéros de téléphone figurent parmi les données que les services de renseignements travaillent à faire correspondre. Le FinCEN peut ainsi "*relier des points entre des individus et des entités ne semblant pas reliés*", a déclaré son porte-parole. Actuellement, le FinCEN détecte chaque mois quelque 1.200 correspondances suggérant une activité financière liée à l'Etat islamique contre 800 en avril, ajoute le porte-parole.

L'utilisation de données financières liées à l'EI n'est qu'une partie de la collecte de renseignement destinée à ajuster les frappes aériennes en Syrie. Il y a également la surveillance aérienne par les drones.

A DOS DE MULET

Un ancien officier militaire du renseignement au fait de ce processus explique que les informations financières collectées par FinCEN doivent ensuite être "*soigneusement vérifiées"* avant que l'armée ne puisse s'en servir pour agir. Le 15 novembre, les avions de la coalition internationale ont détruit 116 camions-citernes transportant du carburant pour le compte de l'Etat islamique près d'Abou Kamal, dans l'est de la

Syrie, 45 minutes après avoir largué des tracts conseillant aux conducteurs de prendre la fuite, déclaré un porte-parole du Pentagone.
Il y a deux semaines, 283 camions camions-citernes supplémentaires ont été visés par les frappes de la coalition. Le 8 novembre, trois raffineries de pétrole près de la frontière avec la Turquie ont été détruites. Avant le mois d'octobre, l'EI gagnait environ 47 millions de dollars par mois (44 millions d'euros) grâce aux ventes de pétrole, selon les estimations du Pentagone. Le Pentagone estime que les frappes de l'opération "Tidal Wave II" ont réduit d'environ 30% les bénéfices de l'EI tirés des ventes de pétrole, déclare un responsable américain de la défense au fait de cette estimation qui n'avait pas été rendue publique.
Reuters n'a pu confirmer ce chiffre en direct. Mais les experts estiment que l'EI dispose de sources de revenus autres que les ventes de pétrole, notamment par l'extorsion de fonds ou les ventes d'antiquités, signale Thomas Sanderson, spécialiste du terrorisme au Center for Strategic and International Studies (CSIS). *"L'argent peut être acheminé à dos de mulet"***,** explique-t-il. "*C'est facile de faire passer des choses par la frontière dans les périodes de privation et de chaos."*
Pour tarir les sources de financement de l'EI, la coopération d'autres Etats sera nécessaire, notamment de la Turquie et de la Russie, estiment les experts. Daech semble avoir tiré les leçons de ce qui s'est passé avec Al Qaïda, qui se reposait sur de riches donateurs. "*L'EI a appris qu'il ne faut pas compter sur un nombre trop grand de ressources extérieures*", estime Thomas Sanderson. "*Les donateurs sont inconstants et sujets aux pressions; or l'EI veut avoir le contrôle*."
Lien : http://international.blogs.ouest-france.fr/archive/2015/11/30/guerre-contre-daech-finance-petrole-15202.html

Cybercriminalité et blanchiment de capitaux sur internet

Le blanchiment d'argent connaît de nouveaux développements depuis l'avènement d'internet. Le présent article fait le point sur cette cybercriminalité en col blanc.
Dans ce cadre, Internet constitue une source d'inquiétudes, dès lors que l'argent criminel y circule très rapidement, emportant différents risques, comme les risques technologiques, l'anonymat, les limitations à l'accord de licences et au contrôle, les risques géographiques et juridiques, et le risque de transactions (financières) compliquées.
Les criminels disposent ainsi, avec Internet, d'un immense « terrain de jeu » pour y développer leurs activités en profitant d'un avantage incontournable d'invisibilité et d'anonymat. Il y a d'infinies possibilités pour gagner de l'argent sans être confronté à ses victimes. Prenons l'exemple des « attaques informatiques » ou des « cyberattaques ». Il est possible de pénétrer des systèmes numériques publics et privés sans dévoiler son identité ou le lieu de la transaction. Le « phishing » constitue une méthode par laquelle on s'empare du code PIN d'une carte de paiement ou d'une carte de crédit, ou même le code d'accès particulier pour accéder à son compte bancaire ou encore le « pharming ». Pensons également à la « cyber-rançon », où une rançon est demandée, afin d'éviter qu'un système numérique ne soit mis hors service. Enfin, il convient de relever les nombreuses informations détournées par des personnes malveillantes et les cas d'usurpations d'identité qui se multiplient notamment sur les réseaux sociaux. L'espace de la Toile est devenu une infosphère où se multiplient et où cohabitent des données personnelles ou publiques, dont l'origine et la véracité ne sont pas certifiées. Et le nombre d'exemples à citer est innombrable.

En ce qui concerne la cybercriminalité, il y a une économie souterraine qui pourvoit aux besoins d'outils, de marchandises et de services pour commettre le cybercrime, et même pour vendre et acheter des biens et des informations volées. Cela s'appelle le « Dark Net ». Il s'agit d'un environnement économique véritable avec des producteurs, des commerçants de marchandises et de services, des fraudeurs et des clients.
Il y a aussi les jeux et les paris en ligne qui ont connu une explosion exponentielle sur la Toile. Un des problèmes en cette matière consiste à contrôler où se trouve le serveur informatique des jeux (question de compétence de contrôle et juridique). Et ce, sans parler de la « monnaie virtuelle » ? La « monnaie virtuelle », telle qu ele bitcoin, se distingue de la « monnaie électronique », du fait qu'elle est créée par un groupe de personnes (physiques ou morales), et non par un État, ou une union monétaire. Cette monnaie est destinée à comptabiliser, sur un support virtuel, les échanges multilatéraux de biens ou de services au sein du groupe concerné. Il s'agit d'un système non régulé, caractérisé par un facteur d'opacité.
En fait il y a deux éléments essentiels qui différencient les deux systèmes. En premier lieu, la monnaie virtuelle peut être utilisée dans le « cyberspace ». Les transactions ne peuvent pas êtres rattachées à une zone géographique déterminée. Les flux ne sont pas détectables : ces « monnaies » sont conçues pour exister en dehors du contrôle d'un organe de régulation. Le système peut être fermé (sans convertibilité avec la monnaie officielle) ou ouvert (avec possibilité de convertir les fonds virtuels en monnaie officielle). En second lieu, la monnaie virtuelle permet aussi des transactions totalement anonymes qui peuvent avoir lieu soit directement entre particuliers, soit par l'intermédiaire de prestataires de services. Tous les acteurs opèrent en dehors du secteur traditionnel des services de paiement. Aucun plafond d'utilisation ou plancher d'identification des utilisateurs ne leur est applicable.
L'ensemble de ces nouvelles possibilités qu'offre Internet ont eu, pour corollaire, la création de multiples possibilités d'y blanchir de l'argent. Parmi les méthodes les plus utilisées, il convient de relever l'emploi des « Payable Through Accounts ». Il s'agit ici de comptes bancaires, dont le titulaire a ordonné que, quand un certain solde a été dépassé sur le compte, ce montant soit directement viré sur un ou plusieurs autres comptes (intérieurs ou internationaux). Une autre variante est le « criss-crossing scriptural », par lequel l'argent est transféré mutuellement entre différents comptes en banque à divers noms à l'intérieur et/ou à l'étranger et cela en combinaison avec des transferts d'argent par des firmes de transferts d'argent.
Actuellement les transferts (internationaux) peuvent être exécutés de différentes manières : par les comptes bancaires traditionnels, l'e-monnaie, les services de paiement Internet ou les services de transferts d'argent traditionnels. Indépendamment du mode de payement, toutes ces manières de transférer de l'argent ont leurs propres vulnérabilités en matière de risques de blanchiment de capitaux. Généralement ces transferts internationaux se déroulent dans la deuxième phase du blanchiment : l'empilement.
Des transferts bancaires, des hommes de paille et des mules bancaires sont des méthodes souvent utilisées pour blanchir des avantages patrimoniaux illégaux obtenus par le « phishing ». Afin de cacher son identité, le criminel peut également contacter plusieurs personnes en leur offrant de l'argent pour utiliser leur compte personnel afin d'y effectuer des transactions. Dans de nombreux cas, les hommes de paille ouvrent un nouveau compte personnel à ces fins et quand la transaction en question a été effectuée, ils déclarent que les fonds leur appartiennent. Les fonds sont ensuite transférés à d'autres comptes intérieurs et/ou étrangers ou retirés en liquides. Souvent

les liquides sont ensuite envoyés par des services de transferts d'argent à l'étranger. Et ainsi la chaîne du papier est interrompue et le criminel a su effacer ses traces et le lien avec le délit sous-jacent est brouillé.
Le recours à des « shell companies », des sociétés qui n'ont pas d'activités (commerciales), aucun actifs ou obligations financières, sont des structures intéressantes pour les « cyberblanchisseurs ». En effet, ces sociétés disposent de différents comptes bancaires étrangers, souvent situés dans des pays offshore. Ces compagnies sont utilisées comme preuve de paiement pour les banques et permettent ainsi d'effacer la trace de l'argent.
Bien que les nouvelles plateformes de paiement en ligne et les monnaies digitales gagnent de plus en plus en influence dans notre vie quotidienne et environnement social, les cybercriminels et les cyberblanchisseurs dépendent toujours de notre système financier et bancaire traditionnel. Les virements (internationaux) sont toujours rapides et efficaces et généralement utilisés au premier stade du blanchiment de même que la cybercriminalité existe en volant de l'argent des comptes en banques des victimes par des techniques frauduleuses.
En outre, le blanchiment d'argent classique dans les casinos est accompagné du blanchiment dans les jeux et paris en ligne, notamment sur les chevaux, le football, etc.
Les plateformes de jeux et de paris en ligne, qui sont vulnérables pour le blanchiment de capitaux et d'autres crimes financiers par la nature de leurs opérations, peuvent servir comme facilitateurs de blanchiment. Les institutions de jeux sont des commerces très actifs en matière de transactions en liquides qui fournissent une série très large de produits et de services financiers, et qui sont semblables à ceux fournis par des compagnies financières et de services de transactions financières. En plus, les compagnies de jeux servent à des clients variés et souvent temporaires dont ils ne savent que très peu. Les logiciels fournis par les organisateurs de jeux et de paris en ligne rendent possible de transférer et d'accumuler de grandes sommes d'argent, et déposer et retirer de l'argent gagné par des virements bancaires ou différents systèmes de paiement électroniques.
Profitant de failles juridiques et de faiblesses des moyens de lutte, le crime organisé diversifie ses activités. Pour cela, il recourt à des moyens sophistiqués notamment aux réseaux numériques pour commettre ses méfaits et masquer ses actes illicites, et ce à l'échelle mondiale. Le crime organisé s'affranchit en effet des contraintes géographiques et juridiques pour saisir des opportunités, notamment avec des opérations de blanchiment. Des efforts sont donc attendus concernant les moyens de lutte, en particulier pour améliorer le recueil, la conservation et l'exploitation de la preuve fondée sur des données numériques.
La lutte contre la cyberdélinquance est un défi non seulement pour l'Europe et chacun de ses Etats-membres, mais pour le monde entier. Face aux possibilités infinies offertes par le numérique et aux risques que cela engendre, un dispositif législatif performant et dynamique est indispensable, qui ne cesse pas de s'améliorer et de s'adapter. Aussi le contrôle et la lutte contre la cybercriminalité doivent être continuellement dynamiques et innovantes. Mais dans ce domaine, rien n'est figé et des pistes demeurent à explorer.
Lien : http://creobis.eu/aml/

Fraude et blanchiment d'argent
La face cachée du financement des échanges internationaux

Le financement du commerce est vital pour l'économie internationale. D'ailleurs, l'Organisation mondiale du commerce (OMC) estime que 80 à 90 % des transactions de commerce international en dépendent. Son fonctionnement doit donc être efficace et résister aux manœuvres des fraudeurs et blanchisseurs d'argent. Les administrations adoptent aujourd'hui les solutions d'analyse et de gestion des données les plus pointues pour contrer ce fléau, mais il est tel qu'elles doivent accélérer considérablement le déploiement de ces solutions si elles veulent contrôler la situation. Une tribune **d'**Alexon Bell, Directeur des solutions de conformité, SAS Fraud & Financial Crime.

Dans le domaine du financement des échanges commerciaux, les fraudes peuvent engendrer des pertes de plusieurs millions d'euros. Les fraudeurs sont motivés par les sommes en jeu, ceux qui pratiquent le blanchiment d'argent y voient un moyen de dissimuler des activités illicites ou criminelles, avec peu de risques d'être démasqués. Tous misent sur la faiblesse des contrôles humains et la dépendance toujours actuelle aux documents papier. Ceci, couplé aux complexités du commerce, à la diversité linguistique et à la multitude d'organisations impliquées, constitue un terreau idéal pour la fraude et le blanchiment.

Malgré une meilleure prise en compte des enjeux, personne ne sait vraiment comment s'attaquer au problème, ce qui n'est guère surprenant compte tenu de la diversité des types de fraudes liées aux échanges commerciaux. L'une des typologies les plus courantes est le double financement : importateurs et exportateurs se mettent d'accord pour produire un chiffre d'affaires factice en vue d'obtenir des crédits, ou pour simuler une opportunité commerciale leur permettant de récupérer chacun de leur côté des financements puis disparaître dans la nature.

Au nombre des autres techniques couramment employées figurent la falsification de comptes, la couverture de directeurs révoqués et la constitution de structures opaques dissimulant des répartitions de capitaux douteuses ou risquées. En matière de blanchiment d'argent, l'approche classique consiste à surfacturer ou sous-facturer des prestations, à livrer des quantités supérieures ou inférieures, voire à expédier des conteneurs vides, dans le seul but de transférer des fonds.

Pour s'attaquer à ces problèmes, les autorités doivent traiter de grandes quantités de données, la plupart étant non structurées et mal intégrées avec les autres informations. Le défi est d'autant plus difficile à relever qu'il est nécessaire d'effectuer une analyse avec un niveau de granularité allant jusqu'à la quantité de marchandises dans chaque conteneur, aux parcours empruntés et à la durée des trajets.

Par ailleurs, la qualité des données dans les transactions internationales est généralement médiocre. De ce fait, les administrations ont du mal à se faire une idée précise des opérations réalisées dans un même pays, et encore plus à cerner leur exposition aux fraudes et au blanchiment d'argent.

La lutte contre ces activités n'a jamais été aisée, et rares sont les organisations qui ont fait véritablement preuve d'efficacité en la matière. Comment doivent-elles s'y prendre pour rectifier le tir ? La première étape consiste à appliquer aux données existantes les dernières solutions de gestion et de nettoyage des données pour créer une vue d'ensemble des informations pertinentes. Il s'agit d'une première phase d'exploration et de découverte, mais une fois les données pertinentes collectées, elle doit être complété des méthodes de qualité des données. Les fournisseurs de solutions

disposent d'outils pour cela, mais cela ne suffit pas. Les banques doivent également prendre leurs responsabilités et résoudre les problèmes que posent encore aujourd'hui leurs données, et déployer des programmes pour collecter des données de meilleure qualité.

Il faut néanmoins rester pragmatique et ne pas viser la perfection. Les entreprises doivent faire avec ce qu'elles ont et utiliser diverses techniques pour améliorer leurs contrôles, en utilisant plus de données et de contexte dès lors que de nouvelles sources peuvent être analysées. Elles doivent miser sur la technologie pour améliorer leurs programmes de conformité et de lutte anti-fraude, et utiliser notamment des techniques de visualisation pour identifier les scénarios, anomalies et valeurs aberrantes.

Les fraudes et le blanchiment d'argent relèvent ni plus ni moins de la tromperie. Pour lutter efficacement contre ces activités, les entreprises doivent exploiter des sources de données tierces qui les aideront à avoir une vision complète de la situation, à lancer une analyse multidimensionnelle de leurs données et à identifier les domaines d'intérêt. Dans ce contexte, l'ancrage des données dans ce qui constitue la réalité : navires, ports, marchandises, compagnies, directeurs, propriétaires, etc… contribue à éclaircir les questions et à fournir des informations pertinentes et réutilisables.

Une fois qu'elles savent « à quoi ressemblent leurs données », les entreprises peuvent commencer à les contrôler et à les analyser, et à instaurer un système de surveillance complet, qui relie efficacement les données internes et celles de sources tierces, tout en offrant une couverture des risques à la fois solide et homogène. L'idéal est de se concentrer sur plusieurs étapes du cycle de vie de la surveillance et du contrôle, tout en ayant la possibilité d'ajouter des informations plus contextuelles au sein d'une plate-forme capable de les traiter efficacement.

Dans ce genre de scénario, il est profitable d'exploiter des technologies d'analyse des big data, comme Hadoop couplé à des outils d'analyse haute performance. De nouvelles fonctionnalités comme l'exploration dynamique des données aident les enquêteurs à analyser et identifier les problèmes. En parallèle, les data scientists ou spécialistes des données peuvent améliorer la détection en adoptant une approche analytique hybride qui consiste à incorporer des règles métier et à interroger des bases de données pour repérer des actes criminels déjà commis. Ils peuvent par la suite utiliser des techniques de détection des anomalies, de text mining et d'analyse des réseaux sociaux pour identifier les infractions jusqu'alors inconnues ou complexes, et établir les relations entre fraudeurs et blanchisseurs d'argent.

En permettant des analyses plus contextuelles, ces technologies facilitent le contrôle des volumes d'alertes. Elles offrent un système d'alerte à plusieurs niveaux et des techniques plus sophistiquées pour les clients à haut risque et/ou les scénarios de faux positifs. Il est ainsi plus facile pour les entreprises de gérer les volumes d'alertes et de déployer une stratégie efficace basée sur les risques.

Grâce à toutes ces fonctionnalités, les équipes en charge de la conformité peuvent repérer les comportements suspects ou inhabituels, prévenir les actes frauduleux et de blanchiment d'argent dans le secteur du financement du commerce. Avec pour finalité de traduire les coupables en justice.

Lien : http://business-analytics-info.fr/archives/7816/fraude-et-blanchiment-dargent-la-face-cachee-du-financement-des-echanges-internationaux/

BlackMarket : 2 hommes arrêtés pour vente de drogue

Deux dealers passant par le blackmarket arrêtés à New York. Ils commercialisaient de la drogue via une importante boutique du dark web.

Selon un rapport de la justice américaine, les deux hommes, Abudullah Almashwali (Area51 – 31 ans – ressortissant yéménite) et Chaudhry Ahmad Farooq (DarkApollo – 24 ans – ressortissant Pakistanais), vendaient de l'héroïne et de la cocaïne via une importante boutique du blackmarket.

139,000 dollars ont pu être gagnés via leur business Internet en vendant pour environ 1.5kg d'héroïne et 72 grammes de cocaïne. Ils se faisaient payer en monnaie Bitcoin (btc, ndr). Ils acheminaient leurs drogues … via les bureaux de poste de New York. Pour connaitre la ville et ses habitudes, les chiens et les « renifleurs » électroniques de drogue sont légions dans les locaux de l'administration de la Grosse Pomme et les services « secrets » d'enquêtes de la poste US sont loin d'être manchots.

Les deux hommes ont été tracés après l'achat de drogue par les policiers. Les colis ont pu être tracés. Les deux dealers risquent 20 ans de prison et 1 million de dollars d'amende en cas de reconnaissance de leur culpabilité. Alpha Bay est l'une de ces nombreuses boutiques du blackmarket qui permettent d'acheter et vendre drogue, arme, données piratées…

Pendant ce temps dans le blackmarket …

… en Allemagne, la police fédérale a mis la main sur quatre dealers locaux qui commercialisaient cannabis, amphétamines, héroïne, cocaïne et ecstasy dans le black market. L'un des individus arrêtés possédaient un porte feuilles bitcoin d'une valeur de 340 000 euros, preuve que son business semblait bien fonctionner. Si une fois de plus les autorités mettent en avant le moyen de paiement Bitcoin, il est évident que le Btc n'est qu'une monnaie parmi d'autres utilisées par les criminels. 11 kg d'amphétamines et 250 grammes d'héroïne ont été saisis, ainsi que 1.425 pilules d'ecstasy et 150 grammes de cocaïne, des cartouches de cigarettes, sans parler d'importantes liquidités en Euros.

La fête aux Bitcoins

L'été 2016 aura été particulièrement communicant sur le sujet du bitcoin. Plusieurs affaires ont mis en avant l'utilisation de cette monnaie dématérialisée et électronique dans des affaires criminelles. L'Australie, l'Allemagne, les USA. Dans ce dernier cas, George Cottrell, a été arrêté par le FBI sur des accusations de blanchiment d'argent de la drogue via des paiement en bitcoins. Les autorités parlent de 62.000 livres. Cottrell n'est pas n'importe qui. Il était en charge de la communication de Nigel Farage, politicien britannique membre du Parlement européen et ancien chef de l'Independence Party (UKIP). George Cottrell agissait dans le dark web sous le pseudonyme de Bill ! Posted On 29 Août 2016.

Lien : http://www.zataz.com/black-market-2-hommes-arretes-vente-de-drogue/#axzz4Ihhqf5mv

Business du Darknet : vendeurs de drogue et d'armes arrêtés

Business du Darknet – Un homme de 31 ans, qui passait par une boutique vedette du blackmarket pour vendre de la drogue, vient d'être arrêté à Vienne par la Bundeskriminalamt. Même chanson, en Allemagne pour un vendeur d'armes à feu.

Le blackmarket, des boutiques ou il est possible de croiser des vendeurs/acheteurs d'armes à feu, de contrefaçons de papier, de places de cinéma pour quelques euros… mais aussi de drogue. Un homme de 31 ans originaire de Vienne avait été arrêté par les « *amis du petit déjeuner* » de la Bundeskriminalamt, la police Autrichienne, en octobre 2015. Connu sous le pseudonyme du vendeur ShanSa, son arrestation vient tout juste d'être révélée (Très certainement en raison d'une infiltration locale par les autorités, NDR). On vient d'apprendre que lors de son arrestation, 2,8 kg d'amphétamine et un kilogramme d'ecstasy avaient été saisis. Lors de l'enquête, il a été découvert que 182 ventes de drogue, sur cinq mois, avaient été orchestrées en Europe, aux États-Unis, en Australie, en Inde et en Autriche. 15.000 euros de chiffre d'affaires, en Bitcoins.

Business du Darknet

… en Allemagne, j'apprends que le procureur général de Francfort vient d'accueillir dans son bureau un ressortissant germano-russe de 26 ans. L'homme, originaire d'Hanovre, est soupçonné d'avoir organisé un trafic d'arme sur Internet. Il est accusé d'avoir vendu et acheté pistolets, fusils, silencieux et munitions via le darknet. Un adepte du blackmarket, des cartes bancaires contrefaites ont été retrouvées à son domicile. L'enquête est toujours en cours.

Comme je vous le révélais ces derniers jours, le business du Darknet n'a jamais été aussi prolifique avec des ventes et des achats d'armes hétéroclites, comme ces tasers cachés dans des téléphones, clés de voiture, de ce pistolet à ultra son, de drogues venues des 4 coins du globe, de faux papiers, mais aussi de bases de données piratées. Les arrestations, elles aussi, se multiplient partout dans le monde, comme à Rouen, en décembre 2015

Lien : http://www.zataz.com/business-du-darknet/#axzz4Ihhqf5mv

BlackMarket : données bancaires piratées pour des conseillers de la Reine d'Angleterre

Des informations privées piratées volées à un ancien conseiller de la Reine ainsi qu'à des avocats, des banquiers, des médecins et d'autres sujets britanniques vendus dans le blackmarket

Je vous le montre souvent, dans le blackmarket, il est possible de trouver de tout. Le black market, ce n'est pas que des sites cachés dans le dark net, le deep web. C'est aussi des sites Internet référencés par Google. Dernier exemple en date : Bestvalid.cc. Un site Russe faisant parti d'une constellation de portails web accessibles en deux clics de souris.

Le cas de Best Valid remue les méninges des autorités britanniques. Ce dernier propose une base de données bancaires de 100 000 comptes de britanniques. Via ce site, des pirates vendent des cartes de crédit et de débit. Jusqu'ici, rien de bien nouveau. 100 000 étant même un chiffre assez banal. Ce qui est moins banal, les

propriétaires des cartes bancaires : un ancien conseiller de la Reine ainsi que des avocats, des banquiers, des médecins et d'autres sujets de sa gracieuse majesté.
Les autorités britanniques tentent de faire fermer ce site en passant par la NCA (National Crime Agency), mais sans résultat pour le moment.
Une boutique étonnante donc, qui permet, via quelques bitcoins, d'acquérir des données bancaires volées. Un journaliste du Times a acheté quelques informations sur BestValid, avec la permission de la victime [Comment pouvait-il connaître la victime avant d'avoir les informations bancaires en main ? NDR]. Les données « acquises » comportaient le numéro de la carte bancaire, son code de sécurité, la date d'expiration, le numéro de téléphone portable et l'adresse postale. Des données qui semblent provenir de piratages de sites Internet tels que Talk Talk.
Lien : http://www.zataz.com/blackmarket-donnees-bancaires-piratees-pour-des-conseillers-de-la-reine-dangleterre/#axzz4Ihhqf5mv

Bitcoin : Prison ferme pour les utilisateurs Russes

Punir les utilisateurs de la monnaie numérique Bitcoin. La Russie propose l'idée.
La Russie propose des peines de prison ferme pour les utilisateurs de la monnaie numérique Bitcoin. Pour le moment, une « idée » qui serait dans les cartons du Kremlin. Selon l'agence de presse Interfax, le ministère russe des finances se prépare à ajouter un amendement au Code criminel local.
Des peines sévères pour les Russes qui utiliseraient le Bitcoin, la crypto-monnaie. Cet amendement ne fait pas dans la dentelle. L'ancienne version de cet amendement condamnait l'utilisateur à un an de « *rééducation par le travail* », bref direction un goulag à casser des cailloux à -40 degrés, et deux ans de prison pour les membres de « groupes organisés ».
Sauf qu'il semble que cette proposition a été considérée comme trop légère par la politique de Poutine. Bilan, les peines ont été intensifiées jusqu'à quatre ans d'emprisonnement, et 8,000€ d'amende, pour un simple utilisateur de la monnaie numérique. Les groupes organisés seront emprisonnés pendant six ans, et 15,000€ d'amende.
Fait intéressant, les partenaires des utilisateurs de Bitcoins, comme les banquiers et les responsables de sociétés de services financiers risquent jusqu'à sept ans d'emprisonnement, 40,000€ d'amende et une interdiction d'exercer durant trois ans.
Le ministère des finances considère que la crypto-monnaie est avant tout exploitée pour des actes malveillants.
Les monnaies dématérialisées sont dans la ligne de mire des autorités et des pirates informatiques. Le concurrent du Bitcoin, le Litecoin, a connu un problème la semaine dernière avec le piratage des forums de LitecoinTalk. Une attaque qui a obligé les administrateurs a demandé aux utilisateurs de changer leur mot de passe le plus rapidement possible !
Lien : http://www.zataz.com/russie-prison-bitcoin/#axzz4Ihhqf5mv

En Floride, le Bitcoin n'est pas de l'argent

En Floride (sud-est des Etats-Unis), le Bitcoin n'est pas considéré comme de l'argent et peut être échangé sans autorisation spéciale, a décidé la justice, octroyant ainsi une victoire aux défenseurs de la monnaie virtuelle.

«Ce tribunal n'est pas expert en économie. Cependant il est très clair même pour toute personne ayant des connaissances limitées dans le domaine que le Bitcoin a encore beaucoup de chemin à parcourir pour devenir l'équivalent des monnaies», écrit dans une décision, rendue le 22 juillet et consultée par l'AFP, la juge Teresa Pooler.

Pour la magistrate, «les bitcoins ne sont pas des instruments monétaires» même s'ils sont de plus en plus utilisés pour régler des transactions financières.

«Cela veut dire que si vous vendez vos bitcoins à quelqu'un d'autre, vous n'avez pas besoin de licence spécifique. C'est comme si vous vendiez vos biens», résume Rene Palomino, avocat de la défense dans cette affaire, la première du genre aux Etats-Unis

En revanche, «si vous vendez les bitcoins pour le compte d'une tierce personne, il vous faut une licence car vous êtes un intermédiaire type Western Union», ajoute le conseil.

Michel Espinoza, un habitant de Miami, était jugé pour avoir vendu en 2013 et 2014, à un policier en civil, des bitcoins pour une valeur totale de 1.500 dollars sur LocalBitcoins, une plateforme dédiée. Ce dernier lui avait dit qu'il comptait utiliser la devise virtuelle pour voler des numéros de cartes bancaires.

Poursuivi pour blanchiment d'argent, son avocat faisait valoir que le Bitcoin n'était pas considéré comme une monnaie à part entière dans l'Etat de Floride.

- tache d'huile -

En lui donnant raison, la juge Pooler a ajouté une corde à l'arc des promoteurs de cette crypto-monnaie, censée accompagner la transformation numérique de la finance et mettre fin au contrôle par les pouvoirs publics et les banques du circuit des transactions financières.

«Les défenseurs du Bitcoin l'ont toujours présenté comme un système s'autorégulant et devant garder un statut à part, une alternative fiable aux monnaies contrôlées par les gouvernements. Ce jugement les conforte», estime Arthur Long, avocat spécialisé au cabinet new-yorkais Gibson, Dunn.

Cette victoire tombe en plein débat sur l'identité de l'inventeur de la monnaie numérique après que l'Australien Craig Wright se fut présenté en mai comme son père putatif avant de faire quelque peu machine arrière.

Créé en 2009 par un ou plusieurs mystérieux informaticien(s) cachés derrière le pseudonyme Satoshi Nakamato, le Bitcoin est une crypto-monnaie, utilisée essentiellement au départ par les «geeks» et l'économie souterraine qui a prospéré dans les pays connaissant de fortes inflations comme l'Argentine et le Venezuela.

Malgré sa forte volatilité, elle a connu son âge d'or lors de la crise grecque car elle est devenue, pour un grand nombre de Grecs, un outil de réserve pour placer leur épargne face aux craintes de retour de la drachme.

Son avantage, selon ses promoteurs, est qu'elle est une monnaie virtuelle mondiale et ne dépend donc ni d'un Etat ni d'une banque centrale.

Dans certains Etats américains, elle est acceptée dans des restaurants et de nombreux magasins alors qu'elle reste interdite en France et en Chine par exemple.

Si le verdict de la juge Pooler s'applique principalement à la Floride, il pourrait faire tache d'huile dans le reste du pays.

«ça va aiguiller d'autres Etats et d'autres tribunaux appelés à se prononcer sur cette question», estime Charles Evans, professeur de finance à l'Université Barry. Cet expert, dont les études affirment que le Bitcoin n'est pas une monnaie à part entière, a été cité par la défense de M. Spinoza.
Les autorités américaines sont partagées sur le Bitcoin: Pour le fisc (IRS), c'est un bien personnel, alors que le département du Trésor l'assimile à une monnaie pouvant être utilisée par des malfrats et autres cartels de la drogue pour blanchir de l'argent sale.
Le régulateur financier de l'Etat de New York (NYDFS) exige pour sa part une licence - Bitlicence - pour effectuer des transactions.
Quelque 15 millions de bitcoins ont été créés dont environ 14 millions seulement sont en circulation, selon les experts. 31 juillet 2016
Lien : http://www.liberation.fr/futurs/2016/07/31/en-floride-le-bitcoin-n-est-pas-de-l-argent_1469567

Drogue, mafia et blanchiment d'argent : Le côté obscur de la pizza

Dans la vie, tout le monde a un côté obscur, même la pizza.
Il y a cinq ans, John Porcello, surnommé « Johnny Pizza », a été arrêté pour escroquerie dans le cadre de la plus grande affaire anti-mafia de l'histoire du FBI.
John Porcello, décrit un jour comme étant « *d'allure un peu rugueuse, mais avec un bon fond* » par un magazine de professionnels de la pizza, était le propriétaire de plusieurs pizzerias dans le Bronx, et le chef réputé d'une grande famille mafieuse.
Johnny Pizza a fini par plaider coupable de prêts usuraires (des prêts à taux d'intérêt frauduleux) et a dû payer une amende de 18 000 $ (environ 16 000 €).
Malgré le fait que ses pizzerias n'aient jamais été directement impliquées dans une affaire de crime organisé, les délits dont il était accusé, tout comme son surnom, rappellent une époque où la pizza et le crime étaient bien plus liés.
Avec l'arrivée de près de 4 millions d'immigrés italiens aux États-Unis au début du XXe siècle, une spécialité culinaire est rapidement devenue l'une des plus répandues du pays : la pizza. Et en même temps qu'elle, une nouvelle manière de gérer les conflits est née : une solution née des codes de conduite des clans de la Sicile rurale, qui a fini par devenir la Cosa Nostra américaine, la mafia.
Avec les années, ces importations italiennes ont été révélées au grand jour, et surtout à l'occasion du procès de la « Pizza Connection » en 1987, quand le procureur en herbe Rudolph W. Giuliani (ensuite devenu maire de New York) a dévoilé un vaste complot criminel impliquant des douzaines de pizzerias dans tous le pays.
Utilisant les pizzerias comme couvertures, les patrons de la mafia sicilienne aux États-Unis sont parvenus à importer 750 kg d'héroïne (d'une valeur estimée à cette époque de 1,6 milliard de dollars, soit 1,4 milliard d'euros) entre 1975 et 1984. Le procès a duré pratiquement deux ans, et fut l'un des premiers à établir une limite claire et irréfutable entre la mafia sicilienne, qui transformait de la morphine turque à Palerme, et la famille Bonanno à New York, qui s'occupait de la distribution dans tous les États-Unis.
Antonio Nicaso est un expert du crime organisé et l'auteur de nombreux livres, notamment *Les mafieux : la culture de la pègre et le pouvoir des symboles, des rituels et des mythes*. J'ai échangé avec Antonio Nicaso sur le lien entre les pizzerias et le

crime organisé, pour mieux comprendre comment des pizzerias modestes avaient pu être à l'origine d'un trafic de drogue à plusieurs milliards de dollars.
« Vous pouvez parvenir au même résultat avec n'importe quel autre type de restaurant, dit Antonio Nicaso, mais à cette époque, c'était plus facile d'acheter une pizzeria et de s'en servir pour vendre de l'héroïne par la porte de derrière. Il y avait des clients qui venaient pour les pizzas, d'autres pour l'héroïne. Et le clan Bonanno, qui se servait beaucoup de pizzerias pour écouler leurs stocks de drogues, était le clan le plus sicilien des Cinq familles, et de loin le plus violent ».
Malgré la complexité du réseau de la « Pizza Connection », et contrairement à ce que l'on pourrait penser, transformer un commerce en organisation criminelle est remarquablement simple. Selon Antonio Nicaso, cela demande juste de la pizza, des substances illicites, et une comptabilité créative. « Une pizzeria peut être un bon moyen de blanchir de l'argent. Imaginez que vous achetez une pizzeria – la plupart sont entre de bonnes mains, bien sûr – mais disons que vous souhaitez améliorer son profit. À la fin de la journée, rien ne vous empêche de créer de faux reçus puisque la majorité des paiements se font en cash ».
« Donc, si vous avez 200 clients un jour donné, un comptable peut modifier les reçus pour qu'ils annoncent 500 clients. Et l'argent que vous ne faites pas en vendant des pizzas, vous pouvez le gagner en vendant de l'héroïne ou n'importe quelle drogue. En d'autres termes, c'est l'une des manières les plus simples de blanchir du fric ».
Mais les pizzerias n'étaient pas seulement une manière fiable de blanchir des revenus criminels. L'énorme attrait et la capacité d'atteinte des livraisons de pizzas signifiaient aussi qu'il y avait un réseau de distribution préexistant qui pouvait être utilisé pour le trafic de drogue. « Ce schéma n'était pas seulement financièrement viable, mais il était aussi très efficace grâce au réseau de distribution déjà établi par les livraisons », explique Antonio Nicaso.
« Avec ce système, on peut livrer une pizza et de l'héroïne en même temps, parce qu'il y a déjà un réseau en place. C'était une manière très créative de s'occuper de l'héroïne et du blanchiment d'argent, avec un commerce légitime comme couverture. Ils ont fini par avoir pratiquement le monopole de l'héroïne en Amérique du Nord, et grâce aux relations qu'ils avaient au Canada, la Pizza Connection s'est même étendue en Ontario ».
Malgré les meilleurs efforts du FBI, le procès de la Pizza Connection n'a pas rassasié l'appétit de l'Amérique pour l'héroïne – ni pour la pizza d'ailleurs. Moins de dix ans plus tard, on a découvert que la célèbre pizzeria « Original Ray's Pizza » sur la 3e avenue à New York était « *le QG d'un important réseau de drogue* », et ce avec la complicité d'une boucherie de Brooklyn et d'un café qui blanchirent des « *dizaines de millions de dollars* » de cocaïne et d'héroïne à eux deux, selon les autorités fédérales.
18.03.2016
Lien : https://munchies.vice.com/fr/articles/drogue-mafia-et-blanchiment-dargent-le-cote-obscur-de-la-pizza

Grande arnaque : « Félicitations, vous êtes recrutés »

Les chômeurs convertis en « cheval de Troie » pour blanchir de l'argent.
Une société ukrainienne a utilisé des citoyens de toutes nationalités (Grecs entre autres) comme partenaires et intermédiaires afin de les impliquer dans une opération de blanchiment d'argent.

Le siège social de cette société est à Kiev, en Ukraine, mais elle détient des bureaux à Tbilissi, à Berlin, à Bucarest et à Londres. Sa « spécialité » est la création d'unités de production dans les pays en développement, l'étude technologique et l'amélioration des systèmes de gestion d'entreprise.
La méthode d'approche des « partenaires potentiels » est simple, surtout qu'actuellement le taux de chômage dépasse les 27 %.
Les personnes travaillant pour la société recherchent sur Internet les CV des chômeurs qui cherchent un emploi dans le domaine marketing. Ensuite, ils communiquent avec eux par courriel et leur proposent une offre d'emploi, qui consiste a transférer des sommes d'argent parvenues de différents pays du monde via Western Union en Ukraine.
Selon la société, les frais pour ce travail s'élèveraient à 1000 euros par mois pour un temps partiel et à 2300 euros pour un temps plein. Outre ce salaire, l'agent recueille 5 % de la somme d'argent qu'il transfère…
…mais les problèmes ont commencé. La banque avec laquelle un individu a coopéré a été averti que son compte serait fermé car il est considéré comme suspect de fraude. Les dirigeants de l'administration fiscale grecque ont annoncé qu'il existe de fortes indications de blanchiment d'argent…
Selon le rapport de l'Office des Nations unies contre la drogue et le crime, le blanchiment d'argent sale était estimé à 1600 milliards de dollars dans le monde en 2009, soit 2,7 % du PIB mondial. Le blanchiment d'argent est au cœur des activités criminelles et représente une menace des plus importantes en termes de sécurité intérieure et de stabilité économique
Lien : http://blog.economie-numerique.net/2014/01/02/grande-arnaque-felicitations-vous-etes-recrutes/

USA:
De grandes banques veulent la fin de l'opacité des sociétés-écrans

Washington (awp/afp) - Plusieurs grandes banques internationales veulent lever l'anonymat des sociétés-écrans aux Etats-Unis, soupçonnées de faciliter l'évasion fiscale et le blanchiment d'argent, affirme un de leurs principaux groupements dans une lettre à des élus américains.
"Nous ne voyons aucune raison de permettre à des entreprises de dissimuler l'identité de leurs propriétaires", indique la missive écrite par The Clearing House, une association réunissant notamment l'américaine JPMorgan, la suisse UBS ou la britannique HSBC.
A l'heure actuelle, des sociétés offshores peuvent être créées aux Etats-Unis sans que soit connu le nom de leurs ayants-droit, compliquant grandement la tache des autorités pour traquer des délits financiers.
Ce mécanisme de plus en plus controversé a été utilisé par le passé pour contourner les sanctions américaines contre l'Iran, abriter les revenus illicites de trafiquants d'armes ou dissimuler le financement d'activités terroristes.
L'administration Obama a lancé une offensive contre cette opacité offshore en exigeant notamment des établissements financiers qu'ils identifient les ayants-droit des sociétés avant d'ouvrir des comptes à leur nom.
Début mai, le président Barack Obama avait d'ailleurs enjoint les banques d'"en faire plus" contre l'évasion fiscale.

Un projet de loi a également été déposé au Congrès qui obligerait à identifier les ayants-droit d'une société au moment de son immatriculation.
Selon la Clearing House qui soutient ce texte, cette loi pourrait "sensiblement aider" à lutter contre le blanchiment d'argent et le financement du terrorisme et faciliterait la mission de surveillance des banques sur les activités de leurs clients.
"A l'heure actuelle, les efforts des banques sont plus compliqués", écrit l'organisation.
09.08.2016.
Lien : http://www.romandie.com/news/USA-de-grandes-banques-veulent-la-fin-de-lopacite-des-societesecrans/727357.rom

La Chine et les USA main dans la main contre la corruption

Les deux pays se sont engagés à intensifier la lutte contre la corruption, le blanchiment d'argent et le financement du terrorisme.
Les tensions entre la Chine et les Etats-Unis sur les libertés individuelles et son expansion territoriale n'empêchent pas la collaboration sur d'autres sujets. Les deux premières puissances mondiales se sont engagées à intensifier la lutte contre la corruption, le blanchiment d'argent et le financement du terrorisme, a déclaré samedi le ministère chinois des Affaires étrangères après une rencontre des chefs d'Etat des deux pays à Washington.
Xi Jinping a entrepris une campagne de lutte contre la corruption en Chine depuis son arrivée au pouvoir il y a plus de deux ans, et les autorités ont entamé des poursuites contre les Chinois qui ont fui à l'étranger, dans le cadre d'une opération visant à rapatrier les responsables soupçonnés de corruption.

Rapatriements de Chinois en fuite

Dans une communiqué de presse, le ministère des Affaires étrangères a publié que "l*es deux parties se sont engagées a intensifier leur coopération effective dans la prévention de la corruption, dans la détection de détournement de fonds publics, l'échanges de preuves, la lutte contre la corruption transnationale, le rapatriement de personnes en fuite et des immigrants clandestins, le contrôle des narcotiques, et la lutte antiterroriste*".
Le ministère chinois de la Sécurité publique et le département américain de la Sécurité intérieure se rencontreront à un "moment opportun" aux Etats-Unis. "*Les deux parties ont salué les récents progrès réalisés dans les rapatriements de Chinois en fuite et d'immigrants clandestins par des vols charter et espère poursuivre cette coopération*", ajoute le communiqué.
La campagne de rapatriement a suscité des inquiétudes en Australie, où la Chine a dépêché des membres des services de sécurité pour faire pression sur des suspects sans prévenir Canberra.
La plupart des pays occidentaux, dont les Etats-Unis, n'ont pas signé de traité d'extradition avec la Chine, où les tribunaux sont contrôlés par le Parti communiste et où l'usage de la force pour extorquer des aveux est considéré comme monnaie courant
Lien : http://www.latribune.fr/economie/international/la-chine-et-les-usa-main-dans-la-main-contre-la-corruption-508499.html

À Los Angeles, scandale de blanchiment d'argent impliquant le film "Le Loup de Wall Street"

La justice américaine s'intéresse à un fonds soupçonné d'avoir détourné des milliards de dollars. Dans cette somme, on trouve notamment les bénéfices du film "Le loup de Wall Street», le film de Martin Scorsese qui racontait justement les aventures d'un trader véreux.

Un fonds d'investissement malaisien du nom de "1MDB" avait pour mission d'investir de l'argent public dans différents projets pour que les bénéfices profitent ensuite à l'économie du pays. Le problème, c'est que grâce à un montage financier, impliquant paradis fiscaux et sociétés écran, des "co-conspirateurs" "comme les appellent le gouvernement américain) ont gardé pour eux des milliards de dollars. Dans "Le Loup de Wall Street", Jordan Belfort, le trader incarné par Leonardo Di Caprio, s'offre un séjour mouvementé à Las Vegas en jet privé. C'est le type de dépenses effectuées par ces co-conspirateurs. Ils ont aussi acheté un tableau de Van Gogh, deux autres de Monet, des résidences de luxe à Beverly Hills. Une partie de cet argent (un milliard au moins) a transité par des banques américaines, c'est pour cela que les Etats-Unis s'en mêlent.

Le film "Le Loup de Wall Street" a été financé par l'argent de "1MDB" à travers la société de production Red Granite Pictures, crée en 2010, un an après le fond d'investissement. C'est Red Granite Pictures qui a fourni l'essentiel des 100 millions de dollars du budget du film. Une fresque de trois heures sur un trader véreux, même réalisé par Martin Scorsese, même avec Leonardo Di Caprio, ce n'est pas forcément le projet sur lequel se jettent les grands studios hollywoodiens. C'était donc de l'argent tombé du ciel. Le film a rapporté près de 400 millions de dollars mais compte-tenu de la provenance douteuse de son budget, la justice américaine veut en saisir tous les futurs bénéfices.

Di Caprio n'est pas directement concerné.

Le dossier de 136 pages monté par la justice américaine ne cite pas directement Di Caprio mais parle d'un acteur vainqueur d'un Golden Globe pour le film. Il aurait participé à au moins l'une des ces spectaculaires fêtes payées avec l'argent de "1MDB". Il connaît deux des trois suspects principaux dans cette affaire. D'abord Jho Low. Cet entrepreneur malaisien et fêtard notoire aurait fait des dons généreux à l'organisation pour la défense de l'environnement qu'a fondée l'acteur. Jho Low aurait mis en contact Di Caprio et un autre suspect, le patron de Red Granite Pictures, Riza Aziz. Et c'est là que ça se complique. Riza Aziz est le beau-fils du premier ministre malaisien Najib Razak qui selon le *Wall Street Journal* aurait aussi profité de cet immense scandale. Mais le gouvernement américain marche sur des œufs. La Malaisie est un allié fidèle dans la lutte contre le terrorisme en Asie. Un allié qu'il s'agit de ne pas trop froisser. 25 juillet 2016

Lien : http://www.franceinfo.fr/emission/en-direct-du-monde/2016-ete/los-angeles-scandale-de-blanchiment-d-argent-impliquant-le-film-le-loup-de-wall-street-25