LA CYBERCRIMINALITÉ BOURSIÈRE

DÉFINITION, CAS ET PERSPECTIVES

ALEXANDRE NEYRET

AUTORITÉ
DES MARCHÉS FINANCIERS
AMF

Résumé

Depuis plusieurs années, et la presse s'en est souvent fait l'écho, la cybercriminalité a envahi notre monde. Le secteur financier et plus particulièrement la sphère boursière n'y échappent pas. Chaque année de nouvelles « cyberattaques » boursières (délit d'initié par le piratage informatique de données confidentielles, diffusion de fausse information financière influant sur le cours de bourse d'une société cotée par la création de « faux » sites Internet ou fausses rumeurs par les réseaux sociaux, manipulation de cours d'instruments financiers par le piratage de terminal de trading…) apparaissent ; il était donc crucial de tenter de dresser un panorama de la cybercriminalité boursière dans le but de mieux comprendre les modes opératoires et les problématiques de potentiels manquements boursiers avec une composante « cyber », auxquels l'Autorité des marchés financiers (dénommée ci-après « AMF ») pourrait avoir à faire face.

Après avoir défini la cybercriminalité boursière et obtenu des ordres de grandeur du coût de la cybercriminalité (en général) et de l'impact d'une cyberattaque sur le prix d'une société cotée, nous avons analysé les différents cas disponibles publiquement, en essayant parfois d'anticiper l'avenir des cyber-manquements d'initié, des cybermanipulations de cours et des cyberdiffusions de fausses informations.

Enfin, une cartographie synthétique accompagnée d'une analyse des facteurs favorisant la cybercriminalité boursière montre l'importance à venir de cette dernière et son impact sur toute la chaîne boursière.

SOMMAIRE

1. Introduction

Dans la 13ème édition de son rapport sur les risques mondiaux en 2018[1], le *World Economic Forum* place les deux risques de cyberattaques et de vols/pertes massifs de données parmi les cinq risques majeurs en termes de probabilité de survenance en compagnie des risques environnementaux comme les catastrophes naturelles, les conditions météorologiques extrêmes et les risques dus aux changements climatiques ; et en 6ème position, en termes de gravité après les armes de destruction massive (sic !), les risques environnementaux et les crises de pénurie d'eau.

1.1. La cybercriminalité et la cybercriminalité financière

De manière plus générale, le changement de paradigme opéré depuis deux décennies consiste à ne plus considérer le risque cyber comme un risque spécifique parmi tant d'autres (entre risque informatique et risque opérationnel), mais bien comme un risque beaucoup plus générique, voire un métarisque[2]; puisque dans notre monde actuel tout est devenu numérique, connecté, et donc potentiellement en proie aux attaques informatiques. L'ère numérique a, d'une part, permis l'exploitation nouvelle de schémas frauduleux anciens, et, d'autre part, facilité l'émergence de nouveaux modes opératoires délictueux. Le terme « cyber » est d'ailleurs utilisé fréquemment, notamment pour qualifier toute sorte de délinquance, qu'il s'agisse de cyberescroquerie ou de cyberterrorisme.

Il n'existe pas de définition juridique communément acceptée de la cybercriminalité. Néanmoins, on peut avancer celle-ci[3] empruntée au Groupe de travail interministériel sur la lutte contre la cybercriminalité : « la cybercriminalité regroupe toutes les infractions pénales tentées ou commises à l'encontre ou au moyen d'un système d'information et de communication[4], principalement Internet ». C'est donc (volontairement) très vaste. Le but poursuivi ici n'étant pas une approche juridique de la cybercriminalité, on ne s'attardera donc pas sur cette définition qui varie selon les pays et les organismes[5], mais on soulignera à nouveau que les systèmes d'information et de communication peuvent être à la fois la cible aussi bien que le vecteur de comportements illégaux.

Afin de limiter notre champ d'investigation, il convient de préciser que nous envisageons la cybersécurité comme la protection des systèmes informatiques d'éventuelles cyberattaques et la cyberrésilience comme la garantie de la continuité et du bon fonctionnement des opérations informatiques en cas d'attaque desdits systèmes. En conséquence, ces deux notions ne seront que très peu abordées, même s'il est évident que la cybercriminalité, la cybersécurité et la cyberrésilience se recoupent. On s'intéressera davantage aux modes opératoires des cyberattaques qu'aux méthodes existantes pour les contrer.

Il y a déjà sept ans, dans son discours du 14 septembre 2011, le directeur adjoint de la Division Cyber du FBI[6] exposait les principales cybermenaces pesant sur le secteur financier américain. Il énumérait ainsi : les usurpations de comptes bancaires, les attaques contre les intermédiaires de la chaine de paiement, les attaques contre les marchés financiers par usurpation des comptes de *trading* ou attaques par Déni de Service Distribué (DDoS) contre les bourses, les vols de cartes de crédit, les attaques contre la banque

[1] Voir bibliographie [1].
[2] Voir bibliographie [161].
[3] Voir bibliographie [2].
[4] On peut aussi comprendre NTIC (Nouvelle Technologie d'Information et de Communication).
[5] Voir bibliographie [3] section I « définition de la cybercriminalité ».
[6] Voir bibliographie [4].

mobile, les vols d'informations confidentielles, l'infiltration et/ou l'infection de la « *supply chain* » et la rupture/brouillage des réseaux de télécommunication.

Depuis, l'actualité n'a pas manqué de lui donner raison, puisque ces dernières années des cybercrimes financiers de grande envergure[7] n'ont cessé d'émerger, comme les vols de cartes de crédit ou le piratage du système de paiement SWIFT[8] (cas ci-dessous). Le risque cyber est d'ailleurs considéré dorénavant comme le risque numéro un par la plupart des institutions financières, notamment les banques et les régulateurs du monde financier.

Cas : **Piratage SWIFT**
Cible : banque
Résumé : La cyberattaque contre la banque centrale du Bangladesh en février 2016 est l'une des attaques les plus célèbres de ces dernières années de par sa sophistication qui allie un savoir-faire financier à un savoir-faire informatique, son important profit et son symbole : une attaque visant une des infrastructures-clés du monde financier et une banque centrale. L'enquête a montré que les cybercriminels avaient patiemment fomenté l'opération puisqu'ils avaient, dès mai 2015, ouvert leur compte aux Philippines[9]. Ils ont ensuite compromis le réseau interne de la banque du Bangladesh, en janvier 2016, puis surveillé l'activité des employés pendant près d'un mois, grâce au logiciel *SysMon* de Windows. Les cybercriminels ont ensuite été capables de subtiliser les *logins* et mots de passe des employés se servant de SWIFT. Ils ont pu ensuite compromettre des serveurs de l'application *SWIFT Alliance Access* avec un *malware* spécifique permettant de contourner les dispositifs de sécurité, d'effectuer des virements et d'effacer les traces des virements SWIFT effectués à la fois dans la base de données mais aussi dans les confirmations imprimées obligatoires des ordres[10]. En usurpant l'identité d'officiels de la Banque Centrale du Bangladesh, des demandes de virement du compte de cette dernière à la Réserve Fédérale des États-Unis à New-York vers des comptes aux Philippines ont été réalisées le 4 février 2016. Le 6 février seulement, les confirmations papier des virements effectués ont été découvertes, permettant de révéler l'ampleur de la fraude et le blocage de trente transactions le 8 février. Parallèlement, des erreurs de frappe dans certains messages (« *fandation* » pour « *foundation* ») ont également éveillé les soupçons de certaines banques et permis d'éviter le virement d'une transaction portant sur 20 millions d'euros. Quatre transactions ont été acceptées pour un montant de 81 millions d'euros.
Profit/Impact: Le profit final s'élève à 81 millions d'EUR pour quatre messages SWIFT. La tentative portait sur un total de 951 millions d'EUR pour 35 messages SWIFT.

1.2. La cybercriminalité boursière

Si l'on appréhende plus facilement la notion de cybercriminalité financière, qu'entend-t-on par la cybercriminalité boursière, sous-ensemble de cette dernière ?

[7] Pour un aperçu plus complet et mis à jour des incidents cyber ayant affecté des institutions financières, voir Voir bibliographie [162]
[8] SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une société privée détenue par ses membres dont l'objet est d'assurer le fonctionnement d'un réseau (baptisé aussi SWIFT par extension) international de communication électronique entre acteurs des marchés, dont notamment les banques, qui s'échangent des messages standardisés relatifs aux opérations financières (ordres d'achat et de vente, confirmations d'exécutions de transactions, instructions de règlement-livraison, ordres de paiement…).
Source : https://www.fimarkets.com/pages/swift_reseau_messages.php
[9] Voir bibliographie [5]
[10] Voir bibliographie [6] et bibliographie [163]

L'Autorité des marchés financiers est plus familièrement connue comme « le gendarme de la bourse ». C'est une autorité administrative indépendante, composée d'environ 450 personnes, qui a pour missions de veiller à la protection de l'épargne investie dans les instruments financiers, à l'information des investisseurs et au bon fonctionnement des marchés . Ces missions sont en partie assurées grâce à ses pouvoirs répressifs, puisque l'AMF dispose du pouvoir d'effectuer des contrôles et des enquêtes, qui peuvent aboutir à des sanctions administratives et disciplinaires[11]. Au sein de la direction des enquêtes et des contrôles, , la direction des enquêtes, dirigée par Laurent Combourieu, compte environ 25 enquêteurs. Ces derniers, dans les cas qui vont nous intéresser dans cette étude, peuvent enquêter sur les trois principaux manquements[12] boursiers :

1. **Les opérations d'initié**, qui consistent, selon l'article L465-1 du Code Monétaire et Financier, pour une personne « *à faire usage d'une information privilégiée en réalisant, pour elle-même ou pour autrui, soit directement, soit indirectement, une ou plusieurs opérations ou en annulant ou en modifiant un ou plusieurs ordres passés par cette même personne avant qu'elle ne détienne l'information privilégiée, sur les instruments financiers émis par cet émetteur ou sur les instruments financiers concernés par ces informations privilégiées* ». L'information privilégiée est définie selon les alinéas 1 à 4 de l'article 7 du règlement (UE) n° 596/2014 mais principalement par : « *une information à caractère précis qui n'a pas été rendue publique, qui concerne, directement ou indirectement, un ou plusieurs émetteurs, ou un ou plusieurs instruments financiers, et qui, si elle était rendue publique, serait susceptible d'influencer de façon sensible le cours des instruments financiers concernés ou le cours d'instruments financiers dérivés qui leur sont liés* ».

2. **La manipulation de cours** qui consiste d'après l'article L.465-3-1 du Code Monétaire et Financier par : « *le fait, par toute personne, de réaliser une opération, de passer un ordre ou d'adopter un comportement qui donne ou est susceptible de donner des indications trompeuses sur l'offre, la demande ou le cours d'un instrument financier ou qui fixe ou est susceptible de fixer à un niveau anormal ou artificiel le cours d'un instrument financier* » et/ou « *le fait, par toute personne, de réaliser une opération, de passer un ordre ou d'adopter un comportement qui affecte le cours d'un instrument financier, en ayant recours à des procédés fictifs ou à toute autre forme de tromperie ou d'artifice.* »

3. **La diffusion d'information fausse ou trompeuse**, qui est principalement définie par l'article L.465-3-2[13] du Code Monétaire et Financier : « *le fait, par toute personne, de diffuser, par tout moyen[14], des informations qui donnent des indications fausses ou trompeuses sur la situation ou les perspectives d'un émetteur ou sur l'offre, la demande ou le cours d'un instrument financier ou qui fixent ou sont susceptibles de fixer le cours d'un instrument financier à un niveau anormal ou artificiel.* »

[11] « Après examen des rapports de contrôle et d'enquête, le Collège peut décider d'ouvrir une procédure de sanction. Il informe alors les personnes en cause des faits qui leur sont reprochés et transmet le dossier à la Commission des sanctions pour instruction et jugement. Sous certaines conditions, le Collège peut proposer aux mis en cause de conclure un accord « de transaction », permettant d'éviter l'ouverture d'une procédure de sanction devant la Commission des sanctions. Si le rapport d'enquête ou de contrôle fait état d'éventuelles infractions pénales, le Collège transmet le dossier au procureur de la République. » d'après le site officiel de l'AMF.

[12] On rappelle très schématiquement qu'il faut réserver le terme délit à l'infraction pénale. Le manquement, sanctionné par la Commission des sanctions de l'AMF, est l'équivalent administratif du délit, sanctionné par le juge pénal. À la différence du délit, le manquement d'initié ne nécessite pas la démonstration d'une intention spéculative.

[13] Mais aussi par l'article L465-3-3 : « 1°/ De fournir ou de transmettre des données ou des informations fausses ou trompeuses utilisées pour calculer un indice de référence ou des informations de nature à fausser le cours d'un instrument financier ou d'un actif auquel est lié un tel indice 2°/D'adopter tout autre comportement aboutissant à la manipulation du calcul d'un tel indice. »

[14] L'article 12.1c) du règlement européen MAR est encore plus explicite : « que ce soit par l'intermédiaire des médias, dont l'Internet, ou par tout autre moyen »

Il est ainsi possible de définir la cybercriminalité boursière comme l'ensemble des manquements boursiers possédant une composante cyber c'est-à-dire « tentés ou commis à l'encontre ou au moyen d'un système d'information et de communication ». On voit que les marchés financiers avec leur technologie complexe et leur interconnexion sont les plus susceptibles d'être la proie de tels cybermanquements boursiers. La criminalité boursière, encore plus que les autres formes de criminalité, ne pourra donc échapper à la « cyberisation ».

À cet égard, dès juillet 2017 dans sa cartographie des risques[15], l'AMF a souligné l'importance des risques de nature cyber avec un focus spécifique sur le sujet. Puis, le 19 février 2018, elle signait une lettre d'intention avec l'ANSSI[16] pour une coopération renforcée dans le domaine de la protection des systèmes d'informations face à la menace cyber qui pèse sur le secteur financier. Enfin, dans son plan stratégique 2018-2022[17], l'AMF rappelait l'enjeu important qu'était devenue la cybercriminalité et sa volonté de développer les nouvelles expertises pour y répondre. Dans les priorités de supervision pour 2019, le président de l'AMF annonçait, le 10 janvier 2019, des contrôles thématiques et courts sur la cybersécurité des sociétés de gestion[18], cette dernière devenant également intégrée aux contrôles classiques[19]. Enfin, l'AMF participe, en règle générale avec la Banque de France et le Trésor, à de nombreux groupes de travail internationaux dédiés à la cybersécurité financière comme le *Cyber Expert Group* du G7, *l'European Systemic Group* de l'ESRB, ou des groupes *adhoc* du *Financial Stability Board (*FSB*)*[20] ou de *l'OICV-IOSCO* (Organisation Internationale des commissions de valeurs)[21] ainsi qu'aux campagnes de remontée d'avis de l'ESMA[22], l'homologue de l'AMF au niveau européen, sur l'amélioration éventuelle des textes de l'UE liés à la cybersécurité financière. Au niveau européen, on note également l'implication de la Banque Centrale Européenne (BCE) avec la publication, en mai 2018, du cadre de tests de pénétration TIBER-EU[23] et, en décembre 2018, de ses attentes en termes de cyberrésilience pour les infrastructures de marché[24].

Les autres régulateurs boursiers ont également fortement réagi à cette menace avec notamment la création d'unités spécialisées de type « cyberunit ». Ainsi la SEC (« *US Securities and Exchange Commission* »), l'homologue américain de l'AMF, a créé en septembre 2017 au sein de sa filière répressive une telle unité en charge des thématiques suivantes : la diffusion de fausse information à travers les médias sociaux et électroniques, les intrusions dans les comptes de *trading*, le *hacking* d'informations privilégiées, les menaces cyber liées aux infrastructures de marché et plateformes de *trading*, les manquements liés à la technologie des registres distribués ou « DLT » (pour *Distributed Ledger*

[15] Voir bibliographie [7]

[16] L'Agence nationale de la sécurité des systèmes d'information (ANSSI) couvre également le secteur financier, dans une approche de défense nationale (application de la loi de Programmation militaire). Le secteur financier constitue en effet l'un des douze secteurs d'activités d'importance vitale (SAIV) sur lesquels l'ANSSI exerce sa compétence nationale. Au sein de chaque SAIV, des opérateurs d'importance vitale (OIV) ont été désignés (la liste est classée au niveau confidentiel défense).

[17] Voir bibliographie [8]

[18] À cet égard, l'Association Française de Gestion (AFG) a publié en octobre 2018 les résultats d'une enquête sur les procédures et les moyens mis en œuvre au sein des SGP relatifs à la cybersécurité. Voir bibliographie [164]
L'article d'Option Finance du 10 décembre 2018 de Séverine Leboucher intitulé « les sociétés de gestion s'arment face au cyber-risque » montre également la prise de conscience de ce secteur.

[19] Les contrôles, qui visent à s'assurer du respect par les entités régulées par l'AMF de leurs obligations professionnelles, sont menés par la Direction des Contrôles et non la Direction des Enquêtes présentée plus haut. Les contrôles courts et thématiques (« SPOT » pour Supervision des Pratiques Opérationnelle et Thématique), par opposition aux contrôles classiques sur un acteur en particulier, sont destinés à évaluer sur un petit échantillon d'acteurs la mise en œuvre de certaines pratiques.

[20] Quia publié en novembre 2018 un « cyber lexicon ». Voir bibliographie [218]

[21] Qui a publié en avril 2016 le très intéressant rapport « Cyber Security in Securities Markets_ An international Perspective » ainsi que « Guidance on cyber resilience for financial market infrastructures » en juin 2016. Voir bibliographie [165] et [166]

[22] Ce document du 10 avril 2019 intitulé « Joint Advice of the European Supervisory Authorities (ESMA, EBA, EOPA) » fournit d'ailleurs un récapitulatif intéressant des textes européens en vigueur relatif à la cybersécurité des acteurs supervisés par ces 3 régulateurs européens dont notamment l'ESMA. Voir bibliographie [167] Annexe C.

[23] Voir bibliographie [219]

[24] Voir bibliographie [220]

Technology)[25] et aux ICO (pour « *Initial Coin Offering* »)[26], les manquements boursiers perpétrés à l'aide du *Dark Web*[27].

Mais quels sont concrètement les cas qui ont marqué la cybercriminalité boursière ? On tentera de collecter et d'analyser tous les crimes et manquements boursiers mondiaux à forte composante cyber de ces dernières années afin d'élaborer un panorama des modes opératoires, des impacts et de l'avenir de cette cybercriminalité boursière.

1.3. Revue de la bibliographie existante

S'il existe beaucoup d'études sur la cybercriminalité en général, il n'existe, à notre connaissance, que très peu de littérature fournissant un panorama complet et détaillé de l'impact du cyber sur la criminalité boursière en tant que telle.

On mettra notamment en avant le site Internet de la SEC « *cyber enforcement actions*»[28] qui recense, sans les analyser, les cas récents traités par sa *cyberunit* (*cf*. *supra*).

Néanmoins, plusieurs sources ont déjà abordé le phénomène de la cybercriminalité boursière, mais souvent sous un angle particulier, généralement celui de la cyberdiffusion de fausses informations et, plus rarement, celui du cybermanquement d'initié ou de la cybermanipulation. Suite à l'affaire Vinci de novembre 2016, sur laquelle nous reviendrons plus en détail, des publications françaises sont apparues telles que « les 3F du *hoaxcrash* : fausse donnée, *flashcrash* et fort profit » de Thierry Bertier[29] qui se concentre principalement sur les effets dévastateurs de la possibilité de diffusion de fausses informations par lnternet couplée avec la rapidité actuelle de réaction des marchés financiers. On trouvera également aussi dans « la cybercriminalité » par Gerard Peliks[30] une explication très détaillée du mécanisme de « *pump & dump* »[31] boursier réalisé à l'aide de *spams* diffusés par des *botnets*. Enfin, l'article de Frédéric Echenne[32] propose une vision encore plus générique des risques d'une circulation non maîtrisée des flux financiers et informationnels sur Internet.

De même, dans son article « *The new market manipulation* », l'auteur souligne, dans un de ses chapitres consacré à la désinformation de masse[33], que les manipulations de cours traditionnelles seront

---

[25] La technologie des registres distribués, ou DLT (*Distributed Ledger Technology*), est un système numérique qui enregistre des transactions d'actifs et leurs détails dans plusieurs emplacements à la fois. Contrairement aux bases de données traditionnelles, la DLT ne dispose pas d'un dépôt de données de référence ni de fonction d'administration centralisée. La blockchain, qui regroupe les transactions sous forme de blocs liés les uns aux autres avant de les diffuser à tous les noeuds du réseau, est sans doute la technologie DLT la plus connue. C'est celle utilisée notamment pour le bitcoin par exemple.

[26] Une ICO (*Initial Coin Offering*) est une méthode de levée de fonds, fonctionnant via l'émission d'actifs numériques échangeables contre des cryptomonnaies durant la phase de démarrage d'un projet.

[27] Le *Dark Web* (ou DarkWeb ou dark web…) est le contenu du World Wide Web qui existe sur des réseaux qui utilisent l'internet public mais seulement accessibles via des logiciels, des configurations ou des autorisations spécifiques (réseaux ami-à-ami de pair à pair, Freenet, I2P et Tor …). Le *Dark Web* forme une petite partie du deep web, la partie du Web qui n'est pas indexée par les moteurs de recherche, bien que le terme « *deep web* » soit parfois utilisé de façon erronée en référence au *Dark Web*.

[28] Voir bibliographie [9]

[29] Voir bibliographie [10]

[30] Voir bibliographie [11]

[31] C'est l'une des manipulations boursières les plus classiques dans laquelle les investisseurs victimes sont encouragés, par des fausses informations très alléchantes diffusées par courriels ou autres, à acheter et spéculer sur une action, souvent peu liquide et faiblement valorisée, dans le but de faire monter très fortement son cours (« *pump* »). Le manipulateur peut alors vendre à profit les actions qu'il a souvent préalablement obtenues pour un coût dérisoire (« *dump* »).

[32] Voir blibliographie [159]

[33] Voir bibliographie [12]

dorénavant remplacées par de nouvelles manipulations à base de cyber-désinformation de masse. Thomas Renault dans « *Market manipulation and suspicious stock recommendations on social media* »[34] montre aussi, quantitativement, que Twitter semble être un vecteur idéal de diffusion de fausse information pour manipuler les cours des sociétés de petite capitalisation.

Enfin, on peut mentionner également le très court mais récent article «*The future of financial crime and enforcement is cyber-based* »[35] dont le titre est assez explicite et qui souligne également à partir de quelques cas bien choisis de cybermanquements d'initié et de cybermanipulations l'importance de la composante cyber pour l'avenir des enquêtes.

Vu la nature même de l'étude consistant en un panorama des cybercrimes boursiers, d'autres références seront également mentionnées dans les parties ultérieures.

1.4. Périmètre, plan et exclusions

Si certaines escroqueries, que l'on pourrait qualifier de cyberescroqueries, puisque la plupart sont commises sur Internet[36], peuvent, sous certaines conditions, entrer dans le champ de compétence de l'AMF, notamment les fraudes relatives aux investissements dans les diamants, le Forex ou encore, plus récemment, les cryptomonnaies[37], nous n'investiguerons pas plus avant cette cybercriminalité qui relève d'avantage de l'escroquerie classique. De manière plus générale, toute la criminalité relative aux cryptomonnaies (intrusion et vol de plateforme d'échanges, fraudes aux ICO, manipulation de cours…) qui mériterait un sujet à elle seule, ne sera pas abordée non plus[38].

Afin de mieux comprendre les enjeux, nous essaierons, dans une première partie, d'obtenir quelques ordres de grandeur chiffrés du coût de la cybercriminalité mondiale, à défaut de pouvoir chiffrer précisément le coût lié à la cybercriminalité boursière, et analyserons, dans le détail, la méthodologie employée pour quantifier ce coût.
Les quatre parties suivantes aborderont chacune les trois grands types de cybercrimes boursiers : les cybermanquements d'initiés, les cybermanipulations de cours, la cyberdiffusion de fausses informations, et rapidement les cyberattaques sur la bourse elle-même[39]. On présentera les cas réels déjà traités par les autorités ainsi que les menaces en cours et les prospectives.

Avant de conclure, on présentera une cartographie récapitulative des cybermanquements boursiers, ainsi qu'une analyse des facteurs favorisant ces attaques dans le secteur financier et boursier.

Il convient de souligner que l'ensemble de cette étude a été réalisé uniquement à partir de données disponibles publiquement, c'est-à-dire soit des cas mis en ligne par les autorités judiciaires (principalement américaines), soit par des articles de presse spécialisée sur l'Internet, comme l'attestent

[34] Voir bibliographie [13]
[35] Voir bibliographie [14]
[36] À cet égard, le rapport « État de la menace liée au numérique en 2018 » du Ministère de l'Intérieur (Voir bibliographie [15]), n'hésite pas à inclure ces escroqueries en ligne dans son panorama de la menace numérique.
[37] Des escroqueries où, grâce à des sites internet alléchant proposant d'investir dans ces actifs « d'avenir », l'argent investi n'est jamais rendu.
[38] Même si les récentes évolutions législatives et notamment la loi PACTE adoptée à l'Assemblée Nationale le 11 avril 2019 offrent un nouveau régime pour les crytpo-actifs en France avec une régulation optionnelle par l'AMF. Voir bibliographie [214]
[39] Même si ce type de crime boursier n'entre pas nécessairement dans les compétences de l'AMF, il paraissait difficile de l'exclure d'une étude intitulée « cybercriminalité boursière ». En revanche, les éventuelles cyberattaques sur les infrastructures liées à la bourse (comme le traitement post-marché) seront exclues du périmètre. On pourra voir par exemple le rapport "*The Evolving Advanced Cyber Threats to Financial Markets* 2018/2019 SWIFT/BAE System publié en novembre 2017" qui présente de manière synthétique quelques risques liés à ces dernières. Voir bibliographie [168]

les références bibliographiques . Le panorama n'est donc certainement pas exhaustif, et ce d'autant plus que beaucoup de cybercrimes restent non détectés ou détectés tardivement[40]. De plus, le temps des enquêtes étant souvent long, les cas présentés ici sont anciens et ne traduisent donc pas nécessairement l'état actualisé de la cybercriminalité boursière.

Enfin, cette étude n'a pas pour vocation d'émettre des recommandations visant à mieux combattre la cybercriminalité ou la cybercriminalité boursière.

[40] On pense bien évidemment aux attaques de type APT (menaces persistantes avancées) supposées placer la persistance dans les systèmes comme priorité et donc aussi la capacité à effacer ses traces.

2. Coût de la cybercriminalité

Ce sujet est intéressant pour trois raisons. Tout d'abord, il permet de mettre en exergue l'importance et l'enjeu du phénomène. Ensuite, une des méthodes d'estimation les plus utilisées de quantification de ce coût s'effectue grâce à l'impact sur le cours des sociétés cotées d'un évènement cyber (attaque ou perte de données), ce qui est en soi un sujet extrêmement important pour un régulateur boursier. Enfin, les incertitudes liées à ce calcul permettent de comprendre le foisonnement de chiffres souvent très différents les uns des autres.

2.1. Les incertitudes

Contrairement à d'autres risques ou à d'autres formes de criminalité peut-être plus facilement quantifiables, il apparait délicat de mesurer précisément le coût d'un évènement cyber (attaque ou perte de données) pour une société touchée (et *a fortiori* de la cybercriminalité dans son ensemble[41]), et ce pour plusieurs raisons dont:

- La rareté des données disponibles. Le phénomène reste relativement récent et les données actuelles le sous-représentent[42]. Beaucoup de sociétés victimes de cyberattaques ont souvent fait le choix[43] de ne pas les révéler ou tardivement[44] (encore faut-il qu'elles les découvrent[45]) par crainte des conséquences réputationnelles ou boursières (*cf. infra*). Néanmoins, les nouvelles réglementations[46] devraient pousser les victimes à plus de diligence et de transparence dans leurs déclarations.
- L'absence de définition unique des coûts à prendre en compte et la difficulté à quantifier certains coûts. Si les coûts directs, tels que les coûts liés à l'investigation forensique, à l'aide juridique, à la remédiation et l'amélioration des systèmes touchés, à l'assistance aux clients, à la perte éventuelle de revenu court terme, semblent connus et facilement quantifiables, en revanche, les coûts indirects comme l'atteinte réputationnelle et son impact sur le revenu, les financements, la perte de clients, comme la reconstruction d'un nouveau système de production ou comme la perte d'informations stratégiques, semblent plus difficile à évaluer. De plus, ces coûts indirects ne peuvent se mesurer que rétrospectivement et souvent après plusieurs années. D'après une étude du FMI publiée en 2017[47], plus de 90 % du coût total d'un évènement cyber proviendrait des coûts indirects dont les pertes de revenu long terme liées au départ des clients pour près de 75 %. Une vision schématique des différents coûts associés à une attaque cyber et empruntée à l'étude « *The Cost of Malicious Cyber*

[41] De manière générale, le coût du crime pour la société est un élément extrêmement complexe à calculer. Si les coûts tangibles directement conséquence du crime apparaissent quantifiables, les coûts de prévention et les coûts sociétaux et liés à la justice semblent plus délicats. De plus les méthodes d'estimation varient également. À titre d'exemple, le coût total du crime aux États-Unis a été chiffré en 2016 entre 690 milliards et 3 410 milliards de dollars soit un facteur 5 d'amplitude. Source : Voir bibliographie [16]

[42] Il est évidemment très difficile d'avoir une estimation exacte du nombre de cybercrimes déclarés par rapport au nombre total de cybercrimes. Certaines sources citent seulement 3% (source : voir bibliographie [17]), d'autres 13 % (source : voir bibliographie [18]), ou 15 % (source : voir bibliographie [19]) voire maximum 20 % (source : voir bibliographie [20]).

[43] Il se peut également que pour certaines entreprises stratégiques, les incidents de sécurité relèvent du secret de la défense nationale et ne soient transmis qu'à l'ANSSI.

[44] On pense évidemment à Uber ou à Yahoo dont la gestion des déclarations relatives aux cyberattaques subies a laissé beaucoup d'observateurs dubitatifs.

[45] On pense bien évidemment aux attaques de type APT (menaces persistantes avancées) supposées placer la persistance dans les systèmes comme priorité et donc aussi la capacité à effacer ses traces. En 2017, une compromission est découverte en moyenne 100 jours après. (source : voir bibliographie [21]). PwC en 2014 avançait même que 71 % des compromissions n'étaient même pas détectées (voir bibliographie [22]).

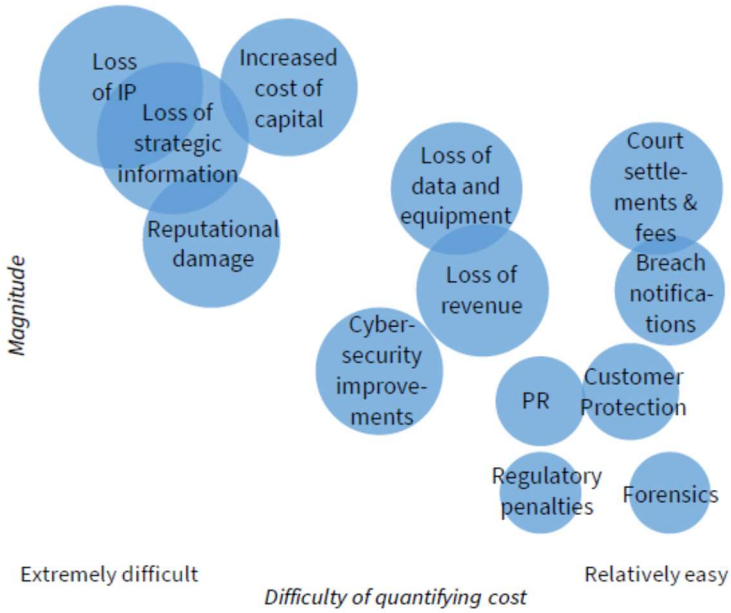
[46] On pense bien entendu aux nouvelles exigences européennes liées au Règlement Général sur la Protection des Données qui imposent une notification à l'autorité de contrôle en cas de violation des données en vigueur depuis le 25 mai 2018; ou aux guidances américaines de la SEC imposant la divulgation des risques de cybersécurité et des cyberincidents, en vigueur depuis 2011 et revues en 2018. Voir bibliographie [169].
A ce sujet, on rappellera l'amende de 35 millions imposée à Altaba (anciennement connue sous le nom de Yahoo !) le 24 avril 2018 pour n'avoir divulgué qu'en 2016 la fuite de données massive subie en 2014. Voir bibliographie [170].

[47] Voir bibliographie [23].

Activity to the US Economy », publiée en février 2018 par le *Council of Economic Advisors*[48] des États-Unis, est reproduite ci-dessous et pointe graphiquement l'importance de ces coûts indirects très difficilement quantifiables.

- La rapidité de l'évolution du monde technologique et donc du risque cyber rendent souvent caduque la pertinence des données historiques.
- L'hétérogénéité des attaques liées à la cybercriminalité, tant dans leur ampleur que dans leur variété.

Figure 1. Cost Components of an Adverse Cyber Event



2.2. Les ordres de grandeur macro

Selon la dernière étude de McAfee et du CSIS en 2018[49], la fourchette globale du coût de la cybercriminalité mondiale a évolué de 345-445 milliards d'USD en 2014 (soit 0,45 % à 0,6% du PIB[50] mondial évalué à 74 100 milliards d'USD) à 445-600 milliards d'USD (soit 0,6 % à 0,8 % du PIB mondial évalué à 75 800 milliards d'USD) en 2017. Il est intéressant de constater que ce coût en pourcentage du PIB régional est élevé et quasiment identique dans les régions développées (Amérique du Nord avec 0,69 % à 0,87 % du PIB, Europe et Asie Centrale avec 0,79 % à 0,89 % du PIB, Extrême Orient et Pacifique avec 0,53 % à 0,89 % du PIB) qui concentrent plus de 80 % du PIB mondial, et nettement plus faible dans les autres régions (Asie du Sud, Amérique Latine et Caraïbes, Moyen-Orient- Afrique du Nord, Afrique Subsaharienne).

Selon l'étude de 2018 citée précédemment « *The Cost of Malicious Cyber activity to the US economy* », le coût de la cybercriminalité aux États-Unis serait estimé entre 57 et 109 milliards d'USD, soit entre 0,31 % et 0,58 % du PIB. On voit donc déjà que ces estimations diffèrent de celles qui sont avancées par l'étude de McAfee et du CSIS avec une fourchette de 0,69 % à 0,87 % du PIB pour l'Amérique du Nord et donc sans doute valable pour les États-Unis.

[48] Voir bibliographie [17].
[49] Voir bibliographie [24].
[50] Pour Produit Intérieur Brut.

Si on applique l'estimation la plus basse (0,31 % du PIB) et la plus haute (0,89 % du PIB) à la France, on obtient, avec un PIB pour 2017 avoisinant 2584 milliards d'USD, un coût global pour la cybercriminalité compris entre 8 et 23 milliards d'USD. D'autres estimations circulent comme 7,1 milliards d'USD[51] ou 4 milliards d'USD[52] pour les entreprises françaises. On voit encore une fois que si l'ordre de grandeur[53] est le même, les variations sont significatives.

Il est intéressant de comparer ce coût de la cybercriminalité mondiale, d'une part au coût des autres formes de criminalité et, d'autre part, à la contribution positive du « cyber » au développement de l'économie mondiale:

- Une étude de 2011 de McKinsey[54] estime que la contribution d'Internet au PIB mondial est d'environ 3 % tandis qu'une étude de 2015 de l'Internet Association[55] l'estime à 6 % du PIB des États-Unis pour 2014. Si l'on rappelle qu'en 2014, le coût de la cybercriminalité avoisinait 0,45 % à 0,6 % du PIB mondial et que les chiffres des États-Unis sont commensurables avec les chiffres mondiaux, on peut estimer la proportion de la cybercriminalité à 10 % de l'activité engendrée par le « cyber ».
- D'après les chiffres fournis par le *Global Financial Integrity* dans son rapport sur le crime transnational en 2017[56], le trafic de drogues mondial représentait en 2014 entre 426 et 652 milliards d'USD et représentait le premier contributeur au crime organisé mondial estimé entre 1600 et 2200 milliards d'USD. L'étude précédemment citée de McAfee et du CSIS en 2018 estime que la cybercriminalité est la troisième activité criminelle la plus lucrative après la corruption et le trafic de drogues, mais c'est indéniablement celle qui touche le plus de monde. Au Royaume-Uni, elle est déjà placée comme l'activité dominante en nombre de crimes déclarés[57]. On peut donc conclure, et surtout au vu de la croissance exponentielle de l'économie digitale, que la cybercriminalité est en passe de devenir la criminalité la plus coûteuse.

Enfin, des études prospectives comme celles de Juniper Research en mai 2017[58] affirment que les pertes de données criminelles coûteront à elles seules plus de 8 000 milliards d'USD sur les 5 ans à venir (soit 1 600 milliards d'USD par an), à cause de l'explosion des objets connectés et de leur faible niveau de sécurité informatique[59]. Ce qui suppose une proportion annuelle du PIB mondial frôlant les 2 % au lieu des « classiques » 0,8 %. La prudence reste donc de mise, car le monde de la sécurité informatique a toujours un intérêt commercial à gonfler l'addition… Néanmoins, il est certain que le taux de croissance annuel de la cybercriminalité pourrait aisément dépasser les deux chiffres.

Il est intéressant d'étudier en profondeur la méthodologie employée par l'étude de 2018 « *The Cost of Malicious Cyber activity to the US economy* » pour obtenir sa fourchette de 0,31 % à 0,58 % du PIB, car elle utilise justement les données issues des marchés financiers pour quantifier le coût de la cybercriminalité et permet de comprendre les incertitudes inhérentes de cette méthode d'estimation et, par extension, de la plupart des estimations du coût de la cybercriminalité. Le postulat de départ de cette méthode basée sur les marchés financiers est le suivant : le cours d'une société cotée étant censé refléter à chaque instant la valeur économique de cette dernière, tout préjudice subi suite à une cyberattaque pourra être déduit en observant la variation de cours éventuelle. La méthodologie suit les étapes suivantes :

[51] Voir bibliographie [25].
[52] Voir bibliographie [26].
[53] Au sens ordre de grandeur physique.
[54] Voir bibliographie [27].
[55] Voir bibliographie [28].
[56] Voir bibliographie [29].
[57] Voir bibliographie [30].
[58] Voir bibliographie [31].
[59] Pour des extrapolations encore plus alarmistes, voire également les 6 000 Mrd$ annuels prédit par la société cybersecurity ventures à partir des 2021. (source : voir bibliographie [32]).

1. Sélection des entreprises cotées ayant été victimes de cyberattaques (ou de fuite de données), depuis janvier 2000 jusqu'à janvier 2017, grâce à une recherche syntaxique sur la base de données du diffuseur d'informations financières Thomson Reuters pour obtenir un échantillon de 186 sociétés affectées par 290 évènements cyber.
2. Définition d'une période d'observation de sept jours après la diffusion de l'information relative à l'évènement « cyber » et d'un benchmark caractéristique (ici le « *market return* » ou taux du marché) permettant d'isoler l'impact de l'attaque cyber sur la variation de cours. On obtient alors une baisse moyenne de 0,8 % de la capitalisation boursière voire une baisse moyenne plus prononcée de 1,01 % si on restreint la période d'étude à 2014-2017.
3. Le calcul du coût global pour toutes les sociétés cotées se fait en multipliant cette baisse moyenne de 1,01 % par la capitalisation totale des bourses américaines (soit 26 600 milliards d'USD à fin 2017) et par la probabilité moyenne annuelle de survenance d'un événement significatif « cyber »[60]. On obtient ainsi 37,2 milliards d'USD. Un raffinement supplémentaire est considéré ici en ajoutant le coût de la propagation de ce préjudice aux autres sociétés économiquement liées[61] soit 9,2 milliards d'USD pour un total de 46,5 milliards d'USD ou 0,17 % de la capitalisation boursière globale.
4. On étend ce pourcentage de 0,17 % à la valorisation de toutes les sociétés non cotées et au secteur gouvernemental pour obtenir 8,7 milliards d'USD et 0,4 milliards d'USD supplémentaires. Enfin on ajoute le coût subi par les individus estimé à 1,5 milliard d'USD d'après une estimation du *FBI Internet Crime Complaint* pour obtenir un total de 57,1 milliards d'USD ou 0,31 % du PIB, la borne basse de l'estimation.
5. Cette estimation peut être revue à la hausse en essayant de tenir compte de la sous-déclaration des évènements cyber chez les sociétés. En remplaçant la probabilité moyenne annuelle de survenance d'un événement significatif « cyber » initiale de 13,85 % par 26,78 %[62], on obtient, en réeffectuant les calculs ci-dessus, une estimation haute de 108,6 milliards d'USD soit 0,58 % du PIB.

Ainsi on note plusieurs éléments essentiels dans cette méthodologie qui peuvent expliquer les incertitudes autour des estimations du coût de la cybercriminalité :

1. Le choix de la méthodologie dite de marché. Il n'est pas évident que le « véritable » coût d'une attaque cyber pour une société cotée soit correctement reflété dans la variation de son cours de bourse. Et ce d'autant plus que l'existence de cycles boursiers influe énormément sur la valorisation des actions (leur cherté relative).
2. Le choix de la sélection de l'échantillon des sociétés cotées victimes d'une attaque. Quelle période temporelle ? Quel type d'attaque ? Où trouver l'information ? L'échantillon est-il assez représentatif, sans biais?
3. Le choix de la fenêtre temporelle d'analyse et du benchmark permettant d'isoler la composante cyber dans la variation du prix « brut ».
4. L'estimation de la survenance moyenne d'un événement cyber qui doit tenir compte du biais de sous-déclaration de ce type d'événement.

[60] Cette dernière est extraite d'une étude de Ponemon datant de 2017 sur les pertes de données et vaut 13,85 %.

[61] En s'inspirant à nouveau du résultat de deux études de Scherbina and Schlusche en 2015 et 2016, les auteurs obtiennent un supplément de 37,2 x (0,8 sociétés liées x0,32 transmission) = 9,2 milliards d'USD.

[62] D'après une étude du CSIS de 2014, lors de l'attaque contre Google en 2010, 34 autres sociétés cotées avaient été également attaquées. Pourtant seule Google avait déclaré l'attaque. Ce 3 % de déclaration effective est à comparer aux 34 incidents cyber effectivement déclarés par des sociétés à Reuters, en 2016, soit potentiellement 1156 sociétés victimes au total en 2016, c'est-à-dire 26,78 % du nombre total de sociétés cotées.

2.3. Les impacts sur les sociétés cotées

Selon une étude réalisée en 2017 conjointement par la société spécialisée CGI et par *Oxford Economics*[63], l'analyse des performances boursières de 65 entreprises de tout secteur et tout continent ayant subi des fuites de données « sévères » ou « catastrophiques » (d'après le *Gemalto Index*), depuis 2013 jusqu'au premier semestre 2016, montre que ces dernières auraient perdu en moyenne 1,8 % de leur capitalisation boursière lors de la semaine suivant la divulgation de ces fuites par rapport à un *benchmark* composé de leur pairs.

L''étude « *The Cost of Malicious Cyber activity to the US economy* » en 2018 montre avec la même fenêtre temporelle d'observation une baisse moyenne de 1,01 % du cours de l'action par rapport au reste du marché (voir *supra*).

De même, dans leur étude « *What is the impact of successful cyberattacks on target firms ?* »[64], les auteurs, pour un échantillon final de 165 cyberattaques sur une période de 2005 à 2017, trouvent une baisse moyenne du cours des sociétés de 1,1 % par rapport au reste du marché dans les cinq jours suivant l'annonce.

L'étude de l'institut Ponemon et de Centrify, en mai 2017[65], sur un échantillon de 113 sociétés, trouve une chute moyenne quasi instantanée (cohérente avec une semaine d'observation mais non explicitée dans les résultats de l'étude) et absolue (pas de *benchmark*) de 5 % du prix de l'action après la divulgation d'une fuite matérielle de données (définie comme une fuite de plus de 50 000 données). Néanmoins, la plupart des sociétés semblent recouvrer leur niveau boursier initial en 45 jours.

Enfin, dans l'article « *Do firms underreport information on cyber-attacks ? Evidence from capital markets*»[66], les trois auteurs, en étudiant un panel de 276 cyberattaques entre 2010 et 2015, trouvent que les cours des sociétés qui déclarent immédiatement être victime d'une cyberattaque subissent une baisse moyenne de 0,7 % (mais non statistiquement significativement différente de 0[67]) dans le mois qui suit l'annonce (dont 0,3% dans les 3 jours qui suivent), tandis que les cours des sociétés dont la cyberattaque est révélée par un tiers subissent jusqu'à 3,56 % de baisse dans le mois qui suit la révélation (dont 1,5% dans les 3 jours qui suivent). Les auteurs confirment également l'intuition que les sociétés ont tendance à ne révéler que les attaques de « faible » envergure pour préserver leur capital réputationnel.

Encore une fois, l'hétérogénéité des critères choisis (au niveau du choix des attaques, au niveau du *benchmark* retenu, au niveau de la fenêtre temporelle et de la période d'étude, au niveau de la communication de l'attaque par la société…) et la faible quantité de données échantillonnées ne permettent pas une conclusion tranchée ; néanmoins, l'ordre de grandeur semble être un impact négatif moyen[68] compris entre 1 % et 5 % dès la divulgation d'une cyberattaque[69].

[63] Voir bibliographie [33].
[64] Voir bibliographie [34].
[65] Voir bibliographie [35].
[66] Voir bibliographie [36].
[67] Cela pourrait s'expliquer par le fait que la période avant 2014 soit une période où le risque cyber n'était pas encore vraiment pris en compte par le marché… (voir bibliographie [17] p10).
[68] On souligne « moyen » ! Qu'on songe à Equifax avec une chute de 18 % en seulement 4 jours (source : voir bibliographie [37]) ou sans doute Uber même si cette dernière n'est pas cotée…
[69] Donc une estimation finale du coût associé à la cybercriminalité, si fondée sur la méthode dite de marché, qui peut varier d'un facteur 1 à 5.

Avec les ravages mondiaux causés par le *wiper* NotPetya[70] en juin 2017, il peut être intéressant d'obtenir des données comptables lorsque les entreprises touchées les dévoilent et de comparer ces données avec les résultats théoriques liés à la variation du cours de bourse et exposés ci-dessus. Ainsi, nous avons pu récolter les données suivantes sur cinq[71] sociétés présentées dans le tableau ci-dessous :

Société	**Impact**	**Résultats sur année 2017**	**Ratio**
Saint Gobain	250 M€ CA	CA à 40,8 Mrd€	0,6 %
	80 M€ résultat d'exploitation	Résultat d'exploitation à 3,028 Mrd€	2,6 %
Fedex	215 M$ résultat	Résultat brut d'exploitation à 5,037 Mrd$ CA de 60 Mrds$	4,2 %
Maersk	250-300 M€ résultat	Cash flows des activités d'exploitation à 2,6 Mrd€ CA à 31 Mrd€	11,5 %
Mondelez	103 M$ de pertes sur les ventes 84 M$ de dépenses en plus	CA à 25,9 Mrd$ Résultat brut d'exploitation à 3,5 Mrd$	0,4 % 2,8 %[72]
Merck	260 M$ de pertes sur les ventes de 2017 125 M$ de pertes sur le Gardasil 200 M$ de pertes sur les ventes de 2018 285 M$ de dépenses en plus	CA à 40 Mrd$ Revenus avant taxes à 6,5 Mrd$	1,4 % 5,8 %[73]

On remarque que le ratio approximatif d'impact sur le résultat d'exploitation annuel oscille entre 2,6 % et 11,5 %. Si l'échantillon est très faible avec des sociétés très hétérogènes et que la spécificité de l'évènement PETYA interdit toute extrapolation, il est quand même remarquable de noter qu'en admettant un ratio « *price to earning* » d'environ 15 qui permet de convertir le résultat d'une société en une valorisation boursière, on obtient un ordre de grandeur de l'impact sur le cours de bourse d'environ 0,5 %[74] relativement comparable aux 1 % avancés précédemment. Ce qui tendrait donc à valider la méthode de marché.

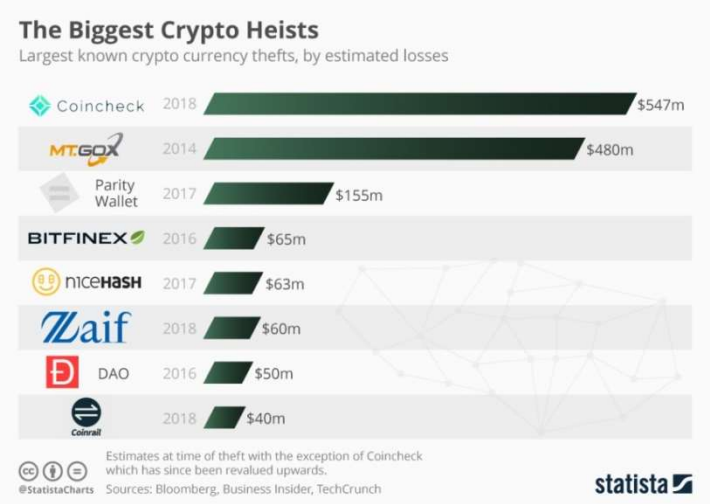
Le développement de cyberattaques de plus en plus puissantes et nombreuses, l'attention renouvelée des investisseurs et du public à cet égard, l'application des nouvelles lois[75] obligeant à la divulgation des cyberattaques ou des fuites de données personnelles avec des sanctions financières extrêmement

[70] Le virus Petya ou plutôt NotPetya de juin 2017, qui ne doit pas etre confondu avec le *ransomware* PETYA de mars 2016, n'était pas un *ransomware* mais un *wiper* (du verbe anglais to wipe qui veut dire « nettoyer » ou « effacer »), un virus dont le seul but est de détruire purement et simplement les données et de rendre les systèmes inopérants.
[71] Voir bibliographie [171].
[72] En prenant en compte très approximativement l'impact des 103 M$ de perte sur les ventes comme 14 millions de profit en moins
[73] En prenant en compte très approximativement l'impact des 585 M$ de perte sur les ventes comme 95 millions de profit en moins
[74] Un ordre de grandeur de l'impact sur le cours du titre de l'attaque est en effet le produit du ratio d'impact divisé par le « *price to earning* » ratio.
[75] Pour un panorama de ces lois : voir bibliographie [38].

conséquentes[76] ainsi que la nécessité de développer des cyber-assurances[77] vont sans doute permettre une explosion des données[78] relatives aux cyberattaques de nature à mieux comprendre le phénomène et décrire plus finement l'impact sur les sociétés cotées.

2.4. Coût de la cybercriminalité financière et boursière

S'il semble admis que les institutions financières et notamment les banques restent la cible privilégiée des cybercriminels, puisque l'argent y est le plus facilement disponible[79], il est difficile d'obtenir une estimation plus détaillée du coût de la cybercriminalité financière en tant que telle. Afin de montrer néanmoins l'importance des sommes en jeu, on pourra mentionner les récents « exploits » du groupe baptisé FIN7 qui aurait volé plus d'un milliard d'USD en 5 ans[80] en cartes de crédit volées, le « piratage » des systèmes de paiement SWIFT qui aurait permis d'engranger plus de 100 millions d'USD[81] à travers six opérations connues dont celle de 80 millions d'USD ayant visé la banque du Bangladesh ou encore les attaques visant les plateformes d'échange des cryptomonnaies dont le total avoisine les 1,5 milliard d'USD, à la fin septembre 2018, comme le montre le graphique ci-dessous intitulé « les plus gros braquages crypto, estimation des pertes des plus gros vols connus de monnaies crypto »[82] :



[76] Que l'on pense aux amendes maximales infligées pour le non-respect du RGPD (GDPR en anglais), applicable à partir du 25 mai 2018, qui pourraient s'élever à 4 % du chiffre d'affaires mondial de la société en question soit une année de dividendes. Le CA global des entreprises du CAC40 sur l'année 2016 s'élève en effet à 1200 milliards pour des dividendes versés de 54,3 milliards (soit 4,5% du CA). On mentionne également l'amende (transaction) de 35 M$ infligée par la SEC le 24 Avril 2018 à Altaba (ex-Yahoo) pour manquement à ses obligations de déclaration des cyberattaques subies en 2014 (Source : voir bibliographie [39]) ou encore l'amende de 700 millions de dollars infligée par la Federal Trade Commission (FTC) à Equifax (cf infra) pour avoir violé les lois américaines en matière de protection de la vie privée (Source : voir bibliographie [216]). Dans un cadre légèrement différent, citons également l'amende record de 5 milliards de dollars infligée toujours par la FTC à Facebook pour l'exploitation par Cambridge Analytica des données personnelles de plus de 50 millions d'utilisateurs à leur insu (Source : voir bibliographie [217]).

[77] L'audition du 15 mai 2019 sur le risque cyber dans les domaines économiques et financiers devant la Commission des finances du Sénat de Christophe Delcamp, directeur adjoint assurance de dommages et responsabilité de la FFA montre clairement que le niveau des primes des cyberassurances en France (80 millions d'euros) reste très limité par rapport aux risques (entre 10 et 20 milliards estimés pour 2018) et que les enjeux de quantification du risque cyber sont véritablement spécifiques.

[78] Dans bibliographie [20], l'application de la PIBR semble déjà avoir permis à la *Data Protection Commission* (DPC) d'obtenir 1184 reporting en un mois contre une moyenne mensuelle de 230 auparavant soit un facteur 5.

[79] Dans voir bibliographie [40] p. 20, le secteur des services financiers paie le coût le plus élevé en terme de cybercriminalité. Dans bibliographie [24] p. 9, les banques restent les cibles favorites des hackers expérimentés. Dans bibliographie [17] p. 20, le secteur financier est de loin le plus touché en nombre d'attaques en 2016.

[80] Voir bibliographie [42], [43], et [44].

[81] Voir bibliographie [6].

[82] Voir bibliographie [172].

Il est encore plus malaisé, au vu du périmètre réduit de la définition de la cybercriminalité boursière, d'estimer le coût de cette dernière, même si les cas présentés dans les parties ultérieures peuvent fournir un ordre de grandeur.

3. Les cybermanquements d'initiés

Comme définie plus haut, une information privilégiée (ci-après dénommée « IP ») est une information précise, non publique et susceptible d'avoir un effet sensible sur le cours du titre de l'émetteur concerné[83]. Or, quoi de plus naturel pour un cyberattaquant que de subtiliser des informations confidentielles sauvegardées dans des systèmes informatiques ? Une fois en possession de cette information, il est en effet facile de la monétiser, soit en achetant le titre avant que son cours ne monte une fois l'information rendue publique, soit en la revendant[84] dans les marchés noirs ou sur des forums spécialisés du *Dark Web*.

Suivant le type d'IP envisagée, un ou plusieurs acteurs peuvent la détenir. Ainsi, dans le cas bien particulier des sociétés dites « biotech », dont la valorisation dépend souvent fortement de l'autorisation donnée par les agences de régulation de mise sur le marché des médicaments qu'elles développent, toute information détenue par ces agences de régulation peut potentiellement être une IP[85].

Dans le cadre plus classique de la préparation d'une opération de fusion-acquisition[86] d'une société acquéreuse sur une société cible, toute une chaîne d'acteurs sera potentiellement au courant : la société acquéreuse, les banques conseils, les cabinets d'avocats, les « *dataroom providers* »[87], les cabinets comptables, les cabinets de consulting, le régulateur boursier, les diffuseurs d'informations financières les agences de relations publiques, potentiellement les agences de traduction (dans le cas d'une opération internationale) voire la bourse elle-même[88]… Les cybercriminels auront tôt fait de tester toute la chaîne afin de choisir le maillon faible comme cible.

La plupart des cas examinés ci-dessous prouvent que la menace peut potentiellement toucher chacun des acteurs.

[83] On pourrait d'ailleurs, même si ce n'est pas notre sujet, se poser la question de la nature des informations privilégiées dans un monde de plus en plus dominé par les « *data scientists* » et le « *big data* ». Si, par exemple, l'analyse des images satellites ou l'utilisation de drones permet d'obtenir quasiment en temps réel le nombre de camions sortant des usines d'une société et donc sa production exacte et par extrapolation les variations anticipées de son chiffres d'affaires, est-ce une information privilégiée ? Voir bibliographie [173]

[84] D'ailleurs il n'est pas non plus nécessaire d'être un cyberattaquant pour revendre son IP et un employé interne à la société peut très bien également revendre son IP, qu'il a sans doute obtenue beaucoup plus facilement ou avec un moindre degré d'intrusion informatique. On retrouve ici la notion anglo-saxonne d' « insider risk »

[85] Voir bibliographie [174]

[86] Pour une discussion plus large sur la cybersécurité et les deals M&A en général, voir l'article de Fireeye « *Unsealing the deal : cyberthreats to mergers and acquisitions persist in a hot market* » (bibliographie [46])

[87] Dans le cadre d'une opération de fusion-acquisition, la *data room* désigne le lieu où l'ensemble des documents juridiques, fiscaux, comptables et économiques d'une société sont mis à la disposition des acquéreurs potentiels et de leurs conseillers pour réaliser l'audit d'acquisition (ou « *due diligence* »), en vue d'évaluer la situation réelle de cette société et la valeur de ses actifs.

[88] Certaines bourses possèdent effectivement un répertoire qui centralise les communiqués officiels envoyés par les émetteurs avant de les rendre publics. Tout dépend en fait du chemin précis de la diffusion de l'information.

3.1. Les cas

Cas : FIN4
Cible : Emetteurs
Résumé : Le cas FIN4 est sans doute l'un des plus emblématiques des cybermanquements d'initié. Dès mi-2013, ce groupe FIN4, baptisé ainsi par *FireEye* dans son rapport détaillé en 2014 « *Hacking The Street, FIN4 likely playing the market* »[89], aurait en effet visé plus de 100 sociétés dont la plupart dans le domaine de la santé et de la pharmacie afin de subtiliser les accès aux boites mails des dirigeants de ces sociétés pour en extraire des informations confidentielles relatives à de potentielles transactions de fusion-acquisition.
Moyens : Leur technique d'intrusion était simple quoique basée sur de l'hameçonnage très élaboré. Aucun *malware* n'était utilisé mais de simples macro VBA sur des documents inclus dans le *mail* d'hameçonnage faisaient apparaître des *pop-up* réalistes demandant à la personne visée de rentrer son *login* et mot de passe Outlook. Afin de légitimer ce mail, dont le contenu montrait la connaissance intime des rouages financiers et du monde de l'entreprise par FIN4, les adresses d'envoi utilisées étaient souvent de véritables adresses mail provenant de sociétés préalablement compromises et dans le même secteur d'activité et les documents utilisés, de véritables documents des sociétés cibles également subtilisés auparavant.
Profit : Il semblerait que la SEC se soit intéressée à cette affaire d'après un article de Reuters du 24 juin 2015[90]. Néanmoins à ce jour, ni les résultats de cette enquête ni donc le profit réalisé ne semblent connus.

Cas : Un technicien IT chez Expedia[91]
Cible : Émetteur
Résumé: De 2013 à 2016, Jonathan Ly, un technicien informatique employé chez Expedia a commis plusieurs manquements d'initié en compromettant les ordinateurs et les boites mail de plusieurs dirigeants exécutifs d'Expedia afin de subtiliser des informations confidentielles relatives aux résultats financiers de la société. Jonathan Ly a ensuite utilisé, à neuf reprises, ces différentes informations privilégiées pour acheter ou vendre des actions Expedia en avance des annonces officielles et publiques diffusées par la société et ainsi réaliser un profit.
Profit : Environ 350 000 USD
Moyens : J. Ly, en tant que technicien informatique, possédait certains droits d'administration. Il a utilisé ces droits pour compromettre le poste de travail d'un technicien informatique senior, dans lequel se trouvait une liste de mots de passe incluant des droits « super administrateur » qu'il a par la suite utilisés pour accéder aux courriels et aux ordinateurs du responsable des relations investisseurs ainsi que du directeur financier à partir de sessions d'autres employés afin de masquer son identité. La compromission des boites mail et des ordinateurs de la société Expedia par Ly a continué même après sa démission en avril 2015, parce qu'il avait gardé un ordinateur portable de la société, lequel lui permettait de conserver son accès à distance, .

Si le cas suivant n'est pas à proprement parler un vol d'IP au sens financier et juridique du terme, il s'en rapproche fortement et permet de mettre à nouveau en exergue la possibilité et la réalité des cyberintrusions chez les émetteurs à des fins de vol d'informations confidentielles et/ou privilégiées. Ainsi de 2008 à 2018[92], deux hackers chinois, membres du groupe APT10, auraient également subtilisé des

[89] Voir bibliographie [47]
[90] Voir bibliographie [48]
[91] Voir bibliographie [49]
[92] Voir bibliographie [175] et [176]

informations confidentielles et des secrets commerciaux provenant de plus de 45 sociétés américaines différentes avant d'être récemment condamnés par la justice. Si leurs motivations penchent vers de l'espionnage industriel et économique étatique, rien ne permet d'exclure une motivation plus économique avec des délits d'initié fondés sur ces informations.

3.1.1. Diffuseur d'information

Cas: **Lohmus**[93]
Cible: Diffuseur d'information
Résumé: En 2005, deux employés d'une société ukrainienne d'investissement *Lohmus Haavel & Viisemann* (Lohmus) se sont frauduleusement introduits dans le site Internet sécurisé du diffuseur d'information financière *Business Wire* pour subtiliser 360 communiqués financiers non encore rendus publics et ainsi effectuer avec profit des transactions d'initiés sur les marchés financiers sur plus de 200 valeurs.
Profit: 7,8 millions d'USD
Moyens: Les deux criminels ont d'abord normalement enregistré leur société Lohmus comme client du site Internet de Business Wire (*Business Wire Connect*). Ce dernier permettait notamment aux sociétés clientes d'envoyer leur communiqué préalable avec l'heure attendue de diffusion publique aux médias par Business Wire. Les deux complices se sont ensuite authentifiés de manière régulière (toutes les deux heures) sur le site et ont utilisé un programme informatique automatisé de type « *spider* »[94] leur permettant de retrouver et de subtiliser tous les communiqués préalables envoyés par les sociétés clientes sur ce site. Les deux criminels ont été notamment retrouvés et confondus, car ils utilisaient la même adresse IP[95] pour leurs transactions financières et pour s'authentifier tous les jours au site *Business Wire Connect* pour en extraire les informations privilégiées.

Cas: **Des hackers ukrainiens compromettent des diffuseurs d'information**[96]
Cible: Diffuseur d'information
Résumé: C'est l'un des cas les plus emblématiques de par sa complexité, le degré de professionnalisme des acteurs, son ampleur et le gain engendré. Entre 2010 et 2015, deux hackers ukrainiens, Ivan Turchynov et Oleksandr Ieremenko[97], se sont introduits dans les réseaux informatiques de deux diffuseurs d'informations financières (MarketWire et PRN) pour y subtiliser près de 100 000 annonces de résultats financiers de sociétés, avant que celles-ci ne soient publiquement diffusées. Turchynov et Ieremenko ont même créé un serveur secret sur lequel des traders pouvaient émettre des vœux concernant les futures annonces à obtenir ainsi que des *shopping lists* d'annonces déjà obtenues. Les traders associés étaient d'une trentaine de nationalités variées (Russie, Ukraine, Malte, Chypre, France, US) et ont utilisé ces informations privilégiées pour effectuer des transactions sur les actions, les options et d'autres instruments financiers d'une douzaine de compagnies différentes avec un gain financier qu'ils partageaient avec les deux hackers (en allant même jusqu'à leur donner accès aux comptes de *trading* en gage de leur bonne foi).
Profits: Les profits réalisés sont supérieurs à 100 millions d'USD.
Moyens: Les moyens utilisés et recensés par l'enquête sont les suivants :
– Attaques combinant un mélange d'hameçonnage et d'injection SQL

[93] Voir bibliographie [50].
[94] Un *spider* est l'autre nom parfois employé pour un *crawler*, c'est-à-dire un programme permettant de répertorier et d'extraire de manière automatisée les informations contenues dans un site Internet. Voir bibliographie [51] pour des exemples de *spider*. Dans notre cas, on peut imaginer que le *spider* était aussi capable de rechercher en plus des fichiers et sites cachés en rajoutant des extensions bien choisies aux adresses trouvées.
[95] Une adresse IP (de « Internet Protocol ») est un numéro d'identification attribué de façon permanente ou provisoire à chaque périphérique relié à l'Internet.
[96]voir bibliographie [52], [53], [54] et [55].
[97] Pour une version plus exhaustive mais peut-être aussi plus romancée de leurs aventures voire bibliographie [177].

- Persistance avec un accès par des portes dérobées (*back-door*)
- Brouillage de leur identité par l'utilisation de mots de passe et de *login* d'employés, utilisation de codes malveillants afin d'effacer les traces de leur attaque et anonymisation de leur adresse IP

Le cas ci-dessus permet également d'illustrer l'existence de réseaux d'initiés, très sophistiqués et très bien organisés (*cf. infra*).

Cas: Oakes[98]
Cible: Diffuseur d'information
Résumé: Entre janvier 2012 et février 2016, M. Oakes, un consultant IT a accédé, sans autorisation, à des informations confidentielles enregistrées dans un ordinateur d'un diffuseur d'information financière à Melbourne et consistant en des recommandations d'achat d'actions par des analystes financiers pour acheter, en 70 occasions, des actions de 52 sociétés différentes de l'indice phare australien ASX avant de les revendre avec profit une fois ces recommandations rendues publiques.
Profits: inconnus.

3.1.2. Banque

Cas: **RIVAS**[99]
Cible: Banque
Résumé: Depuis août 2014 jusqu'à avril 2017, un individu dénommé RIVAS a violé ses devoirs de confidentialité envers la banque de financement et d'investissement qui l'employait en tant que consultant IT dans le département « *Research and Capital Markets Technology Group* », en s'appropriant de manière répétée des informations privilégiées dans le système de suivi des deals/transactions (possibilités de fusions-acquisitions ou de rachat) de la banque et en divulguant ces informations à des connaissances amies qui en ont fait usage sur plus de deux douzaines d'actions en achetant et revendant opportunément ces dernières.
Profit : Au total plus de 5 millions d'USD de profits.

3.1.3. Cabinet d'avocats

Cas: **Hackers chinois et cabinet d'avocats américains**[100]
Cible: Cabinets d'avocats
Résumé: Entre mars et septembre 2015, trois hackers chinois ont pénétré le réseau informatique interne de deux éminents cabinets d'avocats new-yorkais afin d'y dérober des informations privilégiées relatives à des opérations de fusion-acquisition contenues dans les *mails* d'avocats et d'utiliser ces informations pour traiter sur les marchés financiers. En outre, deux de ces hackers ont également essayé, en vain, de pénétrer à 100 000 reprises cinq autres cabinets d'avocats.
Profits: Avoisinant les 3 millions d'USD.
Moyens: Les hackers ont d'abord compromis le compte (*login*/mot de passe) d'un technicien IT. Puis, munis de ce compte, ils ont pénétré le réseau interne de la société et téléchargé un *malware* sur les serveurs qui leur a permis de compromettre le compte d'un autre technicien IT muni de droits super-administrateur et donc d'un accès à toutes les messageries de ladite firme. Afin d'éviter toute détection,

[98] Voir bibliographie [56].
[99] Voir bibliographie [57].
[100] Voir bibliographie [58].

le *malware* était labélisé comme un service de mise à jour de Google Chrome et le téléchargement volumineux de courriels subtilisés masqué pour apparaître comme du trafic réseau normal.

3.1.4. Régulateur boursier

Cas : Intrusion dans le système EDGAR de la SEC
Cible : Régulateur boursier
Résumé : Le 20 septembre 2017[101], la SEC révélait une intrusion datant de 2016 dans son système règlementaire de déclarations EDGAR[102]. Cette intrusion aurait plus spécifiquement concerné la composante « test » des déclarations (par exemple : une compagnie déclarante doit au préalable vérifier le bon format de sa déclaration de résultats financiers avant de la valider définitivement). Les attaquants ont ainsi pu avoir un accès non autorisé à des informations confidentielles et non publiques, qui ont pu servir de base à des manquements d'initié. Cette intrusion a été détectée par un audit commandé par le Président de la SEC dans le cadre d'un plan plus global pour la cybersécurité.
L'enquête, toujours en cours au 21 juin 2018[103], a abouti tout récemment, puisqu'au 15 janvier 2019[104], la SEC a inculpé à nouveau le hacker ukrainien Ieremenko, déjà condamné en 2015 pour s'être introduit dans les réseaux informatiques de deux diffuseurs d'informations financières MarketWire et PRN (*cf. supra*), pour s'être introduit dans la base EDGAR afin de subtiliser plus de 157 résultats financiers, entre mai et octobre 2016, ayant permis à ses complices traders basés en Californie, Russie et Ukraine, de dégager de substantiels profits.
Profit : Au total plus de 4 millions d'USD de profits.

Ce cas est certes très ironique, puisque les cybercriminels se sont servis de la SEC comme source d'information privilégiée, mais il montre encore une fois que la cybersécurité doit être la priorité de chaque acteur de la chaîne financière.

Les cas suivants ne sont pas à proprement parler des cyberattaques visant à subtiliser des informations privilégiées (ou du moins ces cas n'ont pas encore été caractérisés comme tels), mais ils impliquent tous des attaques potentielles et ou des fuites de données qui auraient pu aboutir à une telle finalité.

Cas : Fuite de données du régulateur boursier de l'Oklahoma
Cible : Régulateur boursier
Résumé : En janvier 2019[105], des chercheurs en sécurité informatique découvrent grâce à l'outil SHODAN[106], en libre accès depuis le 30 novembre 2018, des serveurs contenant des données confidentielles du régulateur boursier de l'état de l'Oklahoma (« *Oklahoma Department of Securities* » ou « ODS »). Plus de 3 Teraoctets de données de toute nature datées de 1986 à 2016 contenant des courriels, des déclarations réglementaires, des *logins* et mots de passe d'employés de l'ODS, des dossiers d'enquête (dont des enquêtes menées par le FBI)…
L'ODS a retiré l'accès public à ces serveurs dès le lendemain de la notification par les chercheurs et une investigation forensique est en cours pour déterminer qui aurait pu accéder à quel document.

[101] Voir bibliographie [59].
[102] EDGAR (« *Electronic Data Gathering, Analysis, and Retrieval* ») traite 1,7 million de déclarations réglementaires électroniques par an.
[103] Voir bibliographie [60].
[104] Voir bibliographie [178], [179] et [160].
[105] Voir bibliographie [180].
[106] SHODAN est un moteur de recherche créé en 2009 par John Materly qui référence le résultat de balayages massifs de ports effectués sur le réseau Internet. Il permet grâce à ses nombreux filtres de trouver des objets connectés spécifiques (router, serveur, caméra web, systèmes de contrôle industriel…) et permet d'en détecter certaines vulnérabilités (comme l'absence de mot de passe ou des mots de passe par défaut). Pour une présentation simple de cet outil, voir bibliographie [181].

Cas : FIN7 usurpe l'identité de la SEC
Cible : Régulateur boursier
Résumé : En mars 2017[107], FireEye aurait découvert une campagne d'hameçonnage ciblé, émanant du groupe FIN7, visant des individus en charge des déclarations réglementaires sur la plateforme EDGAR de la SEC chez onze sociétés cotées. L'adresse du *mail* envoyé (EDGAR <filings@sec.gov>) usurpait la véritable adresse de la plateforme tandis qu'un document malicieux Word « *Important_Changes_to_Form10_K.doc* » y était attaché. Une fois ouvert, ce document, à l'aide d'un script VBS, installait une *backdoor* en *PowerShell* (dénommé *Powersource* par FireEye) utilisant les échanges DNS TXT comme canal de communication avec son centre de commande. La finalité de ces attaques n'est pas encore connue.

Un autre cas d'attaque relativement similaire, et qui pourrait relever du même groupe FIN7, a été relevé par Cisco-Talos (ci-dessous) :

Cas : L'identité de la SEC encore usurpée
Cible : Régulateur boursier
Résumé : En octobre 2017, Cisco-Talos[108] dévoilait une nouvelle version d'une attaque DNSMessenger[109] qui utilisait des *emails* d'hameçonnage usurpant l'identité et les codes de la SEC et de sa base réglementaire EDGAR. Ces *emails* contenaient des documents Microsoft Word infectés qui semblaient également officiels (codes, graphismes de la SEC…). Une fois ouverts, ces documents demandaient aux victimes d'autoriser l'activation de liens pour télécharger des fichiers externes, nécessaires à l'affichage complet du document. Si la victime acceptait, du code malveillant était téléchargé et l'infection par *malware* commençait. Ces attaques, hautement personnalisées, complexes, avec l'utilisation de nombreuses techniques de brouillage semblent indiquer un acteur sophistiqué, motivé et persistant. Mais la finalité de ces attaques, n'est pas encore connue.

Une tentative similaire d'usurpation de l'identité de l'AMF dans une campagne de courriels ciblés (adresse en @amf-fr.org au lieu de @amf-france.org), invitant les destinataires à télécharger un document Word renfermant un contenu malveillant , a d'ailleurs été déclarée par cette dernière le 19 octobre 2018[110]. Un article du *Times of Malta* du 25 février 2019[111] établit d'ailleurs un lien possible entre cette campagne de courriels ciblés usurpant l'identité de l'AMF et la cyberattaque de la Banque de Valette (Malte) ayant débouché sur un profit de 13 millions d'euros.

Ce type d'attaque, usurpant l'identité d'un régulateur pour envoyer des mails infectés, semble malheureusement assez répandu, puisque l'homologue australien de l'AMF (« ASIC » pour *Australian Securities and Investments Commission*) en a également souffert[112].

De manière plus générale, les attaques par courriel (« *phishing* » soit « hameçonnage » ou « *spearphishing* » soit « hameçonnage ciblé »), très connues du monde de la sécurité informatique, et même si les tactiques changent et qu'elles se diversifient, resteraient encore parmi les plus privilégiées

[107] Voir bibliographie [61] et [62].
[108] Voir bibliographie [63] et [64].
[109] C'est une attaque qui utilise les échanges DNS TXT pour communiquer entre l'ordinateur infecté et le centre de commande de l'attaque. (voir bibliographie [65]).
[110] Voir bibliographie [182].
[111] Voir bibliographie [183].
[112] Voir bibliographie [184].

par les pirates[113] surtout dans le monde financier[114]. Elles restent simples d'implémentation, peu coûteuses et permettent de cibler facilement le facteur humain, maillon faible de toute organisation, tout en délivrant des *malwares* extrêmement sophistiqués.

3.1.5. Bourse

Cas : Nasdaq OMX[115]
Cible : **Bourse**
Résumé : En février 2011, il a été révélé que des cybercriminels avaient réussi à compromettre une application de la bourse Nasdaq OMX dénommée « *Director's Desk*». Cette dernière permettait le partage d'informations entre membres du conseil d'administration des sociétés cotées (plus de 300 sociétés). Ces informations sont en grande partie des informations privilégiées. Les cybercriminels n'ont *a priori* pas réussi à compromettre la partie « marché » de la bourse mais seulement cette application. Il y a eu beaucoup de spéculation autour de la vraie nature de cet incident.

3.2. Prospectives

3.2.1. Dark Web et insiders

Dans les cas précédents, nous avons vu que la monétisation des informations privilégiées subtilisées se faisait directement par l'emploi de celles-ci sur les marchés financiers. Néanmoins, la cybercriminalité ayant ses propres services, la monétisation de ces IP peut aussi passer par leur revente sur le *Dark Web* .

Dans l'étude "*Monetizing the Insider by RedOwl*" de 2017[116], les auteurs avancent que le *Dark Web* est de plus en plus utilisé par les cybercriminels pour l'achat d'informations privilégiées. Ces informations émanent souvent d'employés de la société concernée par l'IP. Le *Dark Web* est également utilisé pour recruter directement ces employés internes à la société (« *insiders*»[117]) capables de leur fournir un accès au réseau informatique interne de cette dernière, voire de les aider à introduire un *malware*. Ainsi l'activité sur le *Dark Web*, mesurée en nombre de *posts* relatifs aux thématiques susnommées aurait doublé entre 2015 et 2016, et deux exemples de forums très actifs et auto-proclamés très exigeants sur la qualité des informations collectées, aux titres évocateurs comme « *Kick Ass Market Place* » ou « *The Stock Insiders* », fourniraient explicitement des IP monétisables sur le marché boursier.

Il convient aussi de souligner que, même si certaines informations disponibles sur le *Dark Web* ne sont pas en tant que telles des IP, elles peuvent constituer une des briques nécessaires à un cybermanquement d'initié. Ainsi, à titre d'exemple, une société de sécurité informatique anglaise, dans un rapport de janvier 2018, intitulé « *Securing the Law Firm : Dark Web foot print analysis of 500 UK legal firms* »[118], a montré que chacun des 500 plus gros cabinets d'avocats britanniques avait en moyenne 2 000 adresses email avec mot de passe disponibles sur le *Dark Web*. Ces données proviennent en majorité de la perte des données d'un tiers, sur le site duquel on imagine des employés de ces cabinets d'avocats s'être inscrits

[113] Voir bibliographie [185].
[114] D'après un rapport de PhishLabs sur les campagnes d'hameconnage au cours de l'année 2018, les institutions financières sont parmi les organisations les plus touchées et représentent près de 29 % des cibles. Voir bibliographie [186].
[115] Voir bibliographie [66] et [67].
[116] Voir bibliographie [68].
[117] Sur la notion d'insider et d'insider risk, qui a gagné en attention ces dernières années, voir le document très complet de la SIFMA « *Cybersecurity : insider threat best practice guide 2nd edition february 2018* » (voir bibliographie [69]).
[118] Voir bibliographie [70].

avec leur adresse *mail* professionnelle et un mot de passe. Ces données peuvent être à la source d'un hameçonnage ciblé et pertinent sur l'employé du cabinet d'avocat détenteur de l'adresse en question ou d'une attaque de type « *credential stuffing* »[119]. Enfin, si les informations déjà en vente sur le *Dark Web* ne sont pas suffisantes, il semble possible, d'après certains articles[120], d'embaucher directement « à la carte » un hacker pour compromettre un compte *mail* personnel, professionnel ou d'un réseau social d'une cible potentielle.

Ainsi, même s'il est difficile de connaître exactement l'étendue des IP (au sens boursier du terme) disponibles sur le *Dark Web*, il semble légitime pour les régulateurs boursiers de s'armer *a minima* de moteurs de recherche capables d'explorer le *Dark Web* afin d'effectuer une veille et une surveillance, même si les techniques d'infiltration nécessaires dans les forums ne leur sont souvent légalement pas autorisées et que certaines sources avancent que le *Dark Web* perdrait en attrait au profit de media de type Telegram[121].

3.2.2. La cyberattaque comme information privilégiée

Devant l'importance du risque cyber pour les sociétés cotées et surtout de son éventuel impact sur le cours de leur titre (*cf*. *supra*), on pourrait naturellement envisager, non pas l'attaque cyber comme un moyen de dérober une information privilégiée, mais plutôt comme l'information privilégiée elle-même. Ainsi, récemment la SEC a engagé des poursuites contre un dirigeant d'Equifax qui avait utilisé l'information non encore rendue publique de la fuite de données massives pour vendre ses actions (voir ci-dessous).

Cas: **Un cadre exécutif d'Equifax commet un manquement d'initié**[122]
Résumé: Jun Ying, (CIO) d'Equifax et qui devait succéder au CIO global de la compagnie, a commis un manquement d'initié en utilisant sa connaissance d'une perte massive (mais encore confidentielle) de données personnelles subie par Equifax pour vendre ses stock-options avant que la compagnie ne dévoile publiquement dans un communiqué, en septembre 2017, ce cyber-incident, dans lequel 148 millions de citoyens US ont vu leurs données personnelles, comme leur numéro de sécurité social, fuiter.
Profit: En vendant opportunément ces stocks-options, J. Ying a évité une perte potentielle de 117 000 USD.

Pour le lecteur curieux, un rapport très intéressant du GOA (pour « *Government Accountability Office* »[123]) américain analyse d'ailleurs en détail les défaillances internes informatiques d'Equifax ayant permis cette fuite de données massive : existence d'une vulnérabilité critique dont le correctif existant et diffusé seulement quelques jours auparavant n'a pas été complètement mis en place, bases de données insuffisamment segmentées permettant aux attaquants d'accéder directement et facilement à toutes les données, mauvaise configuration de l'équipement de surveillance du trafic réseau à l'origine d'un délai de détection de 76 jours, etc.

[119] Le « *credential stuffing* » est une pratique qui consiste à utiliser les identifiants volés d'un compte sur un site Internet piraté pour essayer d'accéder de manière automatisée (à l'aide de *botnets* notamment) à plusieurs comptes sur divers autres sites Internet. Cette pratique permet ainsi d'accéder à tous les comptes pour lesquels la victime initiale du premier compte piraté utilise le même mot de passe.
[120] Voir bibliographie [71].
[121] Voir bibliographie [72], [73].
[122] Voir bibliographie [74].
[123] L'organisme d'audit, d'évaluation et d'investigation du Congrès des États-Unis chargé du contrôle des comptes publics du budget fédéral des États-Unis. Voir bibliographie [187].

Si le cadre juridique n'est pas nécessairement celui du manquement d'initié, le cas de Muddy Waters avec *Saint Jude Medical*[124] est aussi intéressant, puisque le premier annonçait publiquement que les appareils médicaux du deuxième (notamment les *pacemakers*) présentaient de graves lacunes en termes de cybersécurité et étaient susceptibles de succomber à des cyberattaques (effectuées et filmées par une compagnie de cybersécurité spécialisée dans le domaine médical). Muddy Waters espérait profiter de la chute du cours engendrée par la dissémination publique de cette information pour tirer bénéfice de ses positions à la vente sur *Saint Jude Medical*.

Dès lors, un cybercriminel, ayant au préalable vendu les titres d'une société cible, pourrait commanditer une cyberattaque (*DDoS*, *ransomware*, *malware* ou fuite de données confidentielles…) contre cette société dans le seul but de bénéficier de la chute du cours, une fois la cyberattaque dévoilée.

3.2.3. Les fuites de données, futur terreau des cyberattaques

Le phénomène n'est pas nouveau mais les fuites de données massives de ces dernières années (Yahoo, Uber, Equifax parmi tant d'autres connues ou non) seront sans doute également le futur terreau de cyberattaques où le criminel aura déjà la moitié du travail accompli et pourra, par exemple, utiliser ces informations pour effectuer un cybermanquement d'initié[125], en observant la boite *mail* personnelle (ou professionnelle) préalablement compromise d'un dirigeant ou d'un employé d'une société cotée, ou en usurpant l'adresse *email*, voire l'identité de cette personne, pour lancer une campagne d'hameçonnage à l'allure très légitime. Ainsi, dans une classique mais récente histoire de fraude financière avec usurpation d'identité[126], le criminel avait utilisé des données personnelles provenant d'une importante fuite de données il y a 4 ans… Dans un autre registre, les cybercriminels, dans le cas Shalon (*cf. infra*), avaient utilisé des adresses *email* qu'ils avaient eux-mêmes dérobées comme cibles de leur campagne promotionnelle.

3.2.4. Les indices et indicateurs économiques sensibles

Les indicateurs, indices ou données économiques sont des données extrêmement sensibles pour les marchés financiers. Qui détient, en avance de leur parution officielle, ces informations, détient une information privilégiée, bien entendu relative à l'instrument financier concerné.

Par exemple, l'indice de confiance des ménages américains MCSI (pour « *Michigan Consumer Sentiment Index* »), très observé aux États-Unis pour son impact sur les indices boursiers, est calculé par des chercheurs de l'Université du Michigan[127], puis envoyé à *Thomson Reuters* qui le diffuse auprès de ses clients par ses propres canaux de transmission. La question de la (cyber)sécurité en amont de cet indice peut se poser. Ces indicateurs peuvent être calculés par des acteurs externes privés, comme ici l'Université de Michigan[128], mais aussi par des acteurs étatiques. Ainsi, les chiffres officiels du chômage en France sont calculés par Pôle Emploi et la DARES (service statistique du ministère du Travail), et ils ont

[124] Voir bibliographie [75].
[125] De la même façon des intrusions de compte de trading seront également facilitées ainsi que la diffusion de fausse information…
[126] Voir bibliographie [76].
[127] Voir bibliographie [77]. À ce propos, l'agence Thomson Reuters, en partenariat avec l'Université, offrait la possibilité à ses meilleurs clients d'obtenir le fameux indice en avance des autres. Cette pratique a été suspendue par la suite puisqu'elle donnait un avantage indu aux meilleurs clients, en l'occurrence une information privilégiée. (source : voir bibliographie [78])
[128] Par exemple, on a aussi le *Consumer Confidence Index* calculé par le Conference Board et le PMI (aussi appelé ISM Index) calculé par l'Institute of Supply Management parmi tant d'autres.

un fort impact sur la valorisation de certains instruments cotés comme les obligations françaises, le CDS[129] souverain français ou l'indice CAC40. Il n'est pas certain que le protocole de production et de transmission de tous ces indicateurs ait pris en compte la possibilité d'une intrusion dans leur système informatique. Un exemple finlandais du 21 novembre 2018[130], avec des cyberattaques sur un site officiel hébergeant des données potentiellement sensibles du Ministère des affaires économiques et du travail, montre que ces scénarios ne sont pas de la fiction. Ils le sont d'autant moins que nombre de ces données potentiellement sensibles proviennent d'organismes publics, dont les systèmes d'information semblent particulièrement menacés à travers le monde, du fait de l'obsolescence des technologies existantes ainsi que du futur départ à la retraite des responsables en charge de la maintenance de ces systèmes[131].

Ce sont seulement quelques exemples parmi tant d'autres. Pour chaque classe d'actifs (actions, crédit, taux d'intérêts, taux de change, matières premières, énergie, immobilier…), il existe en effet une multitude d'instruments financiers, dont le prix varie en fonction de plusieurs données. Un exercice plus exhaustif de cartographie à l'échelle de chaque régulateur boursier pourrait être utile pour définir la liste des indicateurs et données clés susceptibles d'être la cible de cybermanquements d'initié, en fonction du niveau de sécurité de leur mode de production et de diffusion.

3.2.5. Nouveaux points d'entrée

Avec le développement des ordinateurs portables, des *smartphones* et maintenant des objets connectés (près de 8,4 milliards en 2017 et presque 20,4 milliards en 2020[132]) et la migration massive des entreprises dans le *Cloud*, les points d'accès potentiels pour les cybercriminels sont de plus en plus nombreux : les voyageurs d'affaires, dont les cadres dirigeants détenteurs d'informations confidentielles font partie, sont une porte d'entrée idéale pour les cybercriminels si les connexions à distance ne s'effectuent pas de manière sécurisée[133], les employés dont les équipements mobiles sont utilisés à la fois à des fins personnelles et professionnelles avec le risque de télécharger des *malwares* sur des sites compromis ou sur les réseaux sociaux[134]. Certains dangers comme celui des connexions au réseaux Wi-Fi publics/ouverts, dans les hôtels par exemple, sont également connus.[135]

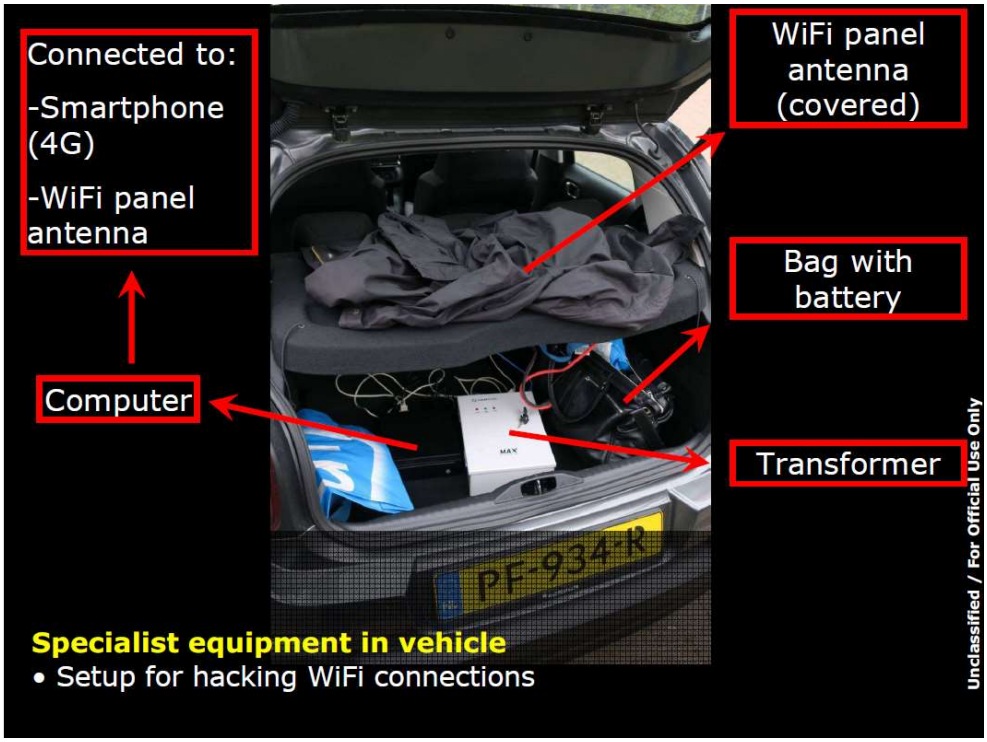
Mais *quid* des possibilités offertes par les nouveaux comportements numériques des entreprises dont de plus en plus de services (comme les messageries notamment avec *Microsoft Office 365*) sont concentrés dans le *Cloud* souvent avec une seule couche d'authentification centralisée?[136]

Quid également des possibilités de chargement rapide des batteries dans les lieux publics ou autres par connexion USB[137] ? De même, les vulnérabilités offertes par des objets connectés comme les montres ou autres gadgets que l'on branche sur l'ordinateur le sont peut-être un peu moins, tout comme les objets connectés commandés à la voix dont certains ont montré qu'ils pouvaient enregistrer des conversations

[129] CDS pour « Credit Default Swap » : produit dérivé de crédit permettant de se couvrir contre la survenance d'un défaut de paiement contre l'échange d'une prime. Un taux de chômage plus élevé que prévu aurait tendance à augmenter la prime visant à s'assurer contre un défaut de paiement de l'État français.
[130] Voir bibliographie [188].
[131] Voir bibliographie [189].
[132] Voir bibliographie [79].
[133] Voir bibliographie [80].
[134] Selon un rapport de l'entreprise de cybersécurité Bromium, la cybercriminalité impliquant les réseaux sociaux est en effet en forte hausse. Le rapport indique qu'une compromission d'entreprise sur cinq a un lien avec un maliciel distribué par un réseau social. Voir bibliographie [190].
[135] Voir bibliographie [81].
[136] Voir bibliographie [191] et bibliographie [192].
[137] Voir bibliographie [82].

à notre insu[138]... Même l'assistant expert vocal des smartphones semble être susceptible d'être compromis[139]. Les éditeurs de solution anti-virus les plus connus, dont sont friands les systèmes de sécurité informatique, regorgent d'informations sur ces derniers et la récente controverse[140] sur les risques de sécurité posés par les produits *Kaspersky* qui pourraient être exploités par des cyberacteurs russes malveillants pour compromettre les systèmes d'informations fédéraux américains le prouve.

De manière plus générale, tous les moyens utilisés pour des campagnes de cyberespionnage sont également pertinents : en témoigne la tentative d'espionnage russe du 4 octobre 2018 mise à nue par les Pays Bas[141], où des équipements d'interception du trafic Wi-Fi avaient été découverts dans le coffre d'une voiture banalisée garée près du parking du bâtiment cible néerlandais (cf. photo ci-dessous[142]). Une telle campagne pourrait également servir au vol des IP.



On pense également à la controverse d'octobre 2018[143] accusant la Chine d'espionnage économique au détriment des grandes sociétés américaines, grâce à l'installation de micropuces produits en Chine dans les serveurs informatiques de ces sociétés .

Bref, si beaucoup d'acteurs du monde boursier peuvent être la cible de cybercriminels à la recherche d'IP, les possibilités d'intrusion offertes par les nouvelles technologies sont de plus en plus nombreuses et la surface d'attaque en est démultipliée d'autant.

[138] Des Google Home ou des Amazon Alexa disposés dans des bureaux d'exécutifs pourraient facilement obtenir des informations privilégiées…
[139] Voir bibliographie [83].
[140] Voir bibliographie [193].
[141] Voir bibliographie [194].
[142] Voir bibliographie [195]. On distingue sur la photo une antenne WiFi recouverte sur le hayon arrière et dans le coffre, un sac avec une batterie, un transformateur et un ordinateur relié à un smartphone (4G) et à l'antenne WiFi
[143] Voir bibliographie [196] et [197].

4. Les cybermanipulations de cours

Il existe de nombreuses variétés de manipulations de cours mais, à titre d'exemple, pour manipuler « artificiellement » le cours d'un instrument financier à la hausse[144], vous avez plusieurs possibilités, non mutuellement exclusives, :

1) Acheter l'action de manière agressive à des prix de plus en plus élevés, ce qui va mécaniquement augmenter le cours (un peu à la manière d'une enchère) ;
2) Émettre des ordres d'achat de taille significative n'ayant pas vocation à être exécutés, pour signaler un fort intérêt acheteur au reste du marché et ainsi l'entraîner à ajuster ses cotations à la hausse (« *layering/spoofing* »).
3) Diffuser de fausses rumeurs visant à entraîner le marché à spéculer à la hausse sur ce titre.

Lorsque le criminel emploie la stratégie 1 et/ou 3 (« *pump* »), avant de revendre avec profit les titres acquis au préalable à faible coût (« *dump* »), on retrouve le schéma manipulatoire bien connu « *pump&dump* ».

La potentielle composante cyber est évidente. La compromission des comptes de *trading* va permettre la mise en place des stratégies 1 et 2 tandis que le vecteur de diffusion de la stratégie 3 est très largement cyber ou numérique (*emails*, faux-site, réseaux sociaux). Cette stratégie 3, en tant que telle, est présentée en détail dans la partie cyberdiffusion de fausses informations même si elle peut également relever de la cybermanipulation de cours.

Les cas présentés ici sont en majorité des cas de « *pump&dump* » où des comptes de *trading* de particuliers ont été compromis.

4.1. Les cas

4.1.1. Intrusion de comptes de trading de particuliers

Cas: **Willner**[145]
Résumé: De septembre 2014 à aout 2016, Joseph P. Willner a manipulé le cours de plusieurs actions à l'aide des transactions effectuées par son complice à partir de plus de 110 comptes de *trading* usurpés pour en tirer un profit sur son compte de *trading* personnel. J. Willner partageait ensuite la moitié de ses gains avec son complice.. Dans un échange de messagerie instantanée entre les deux escrocs, les enquêteurs ont retrouvé la phrase culte : « **Le trading légal est trop difficile** ». Les deux exemples ci-dessous permettent de mieux comprendre les manipulations potentiellement utilisées.
Le 10 avril 2015, après la clôture du marché, Willner entre un ordre de vente à découvert de 537 actions de *First Community Corporation* ("FCCO") à un prix limite de 14,88 USD par action soit un prix bien supérieur au prix de clôture de 11,64 USD. En même temps, son complice usurpe le compte de *trading* d'une victime et place un ordre d'achat pour 537 actions avec un prix limite à 14,88 USD. Les deux ordres sont exécutés l'un en face de l'autre. Quelques instants après, Willner place un ordre d'achat de 537 actions à 9,4 USD, soit un prix bien inférieur au prix de clôture de 11,64 USD et son complice place l'ordre de vente inverse sur le compte de la victime. Ainsi Willner a réalisé un profit de 2942 USD tandis que la victime en a perdu autant.

[144] L'inverse est bien évidemment valable pour une baisse.
[145] Voir bibliographie [84].

Le 17 mai 2016, pendant les heures d'ouverture de bourse, un complice de Willner utilise le compte d'une victime pour acheter un grand nombre d'actions *Lawson Products, Inc.* ("LAWS") à un prix toujours plus élevé, ce qui cause mécaniquement la hausse du cours de l'action LAWS. Willner vend alors à découvert l'action à ce prix artificiellement haut tandis que son complice utilise toujours le compte de la même victime pour cette fois vendre cette action jusqu'à ce que son prix baisse de manière importante. Willner rachète alors l'action à bas prix et gagne ainsi la différence.

Profits : au moins 700 000 USD pour le trader mais une perte de 2 millions d'USD pour les sociétés de courtage touchées.

Moyens : Les moyens de compromission des comptes des victimes ne sont pas connus. Willner avait pris soin d'échanger avec son complice par messagerie instantanée sur Internet avec un pseudonyme. Néanmoins, il accédait à cette messagerie avec l'adresse IP de son véritable domicile[146].

Cas: **Mustapha**[147]

Résumé: En avril et en mai 2016, Idris Dayo Mustapha a compromis de nombreux comptes de *trading* de particuliers et utilisé ces derniers pour traiter avec profit sur son compte personnel. Le schéma manipulatoire est semblable à celui qui est présenté plus haut avec un achat agressif d'actions sur les comptes des victimes pour fixer le cours à un niveau artificiellement haut et vendre, par la suite, les actions avec profit pour le compte du criminel.

Profits : 68 000 USD de profit pour Mustapha et, au moins, 289 000 USD de pertes pour les victimes.

Moyens : Les comptes auraient été compromis grâce à l'accès à un compte administrateur. Mais la compromission de ce dernier n'est pas détaillée.

Cas: **Le trader letton**[148]

Résumé: De juin 2009 à août 2010, un trader letton, Igors Nagaicevs, a manipulé le prix de plus de 100 actions du NYSE et du NASDAQ, grâce à la compromission de comptes de *trading* de particuliers. Le mode opératoire est relativement similaire aux précédents : prise de position à l'achat (ou à la vente) sur le compte personnel du trader, manipulation du cours à la hausse (ou à la baisse), grâce aux achats nombreux et agressifs provenant des comptes des victimes, et enfin débouclage avec profit de la position initiale sur le compte personnel du trader avec des ventes (ou des achats) à des prix artificiellement élevés (ou bas). Le trader réussissait souvent à faire son aller-retour en 15 à 20 minutes seulement, mais il était pourtant responsable (en incluant le compte des victimes) de plus de 50 % du volume quotidien échangé. Il a effectué ces manipulations plus de 150 fois en 14 mois.

Profits : 850 000 USD en profits et plus de 2 millions d'USD de pertes pour les clients.

Moyens : Non divulgués.

Cas: **BROCO** [149]

Résumé: D'août 2009 jusqu'à décembre 2009, Valery Maltsev, président de *Broco Investment*, a manipulé le cours d'au moins 38 actions grâce à la compromission de comptes de *trading* de particuliers. Le mode opératoire est identique à celui du trader letton ci-dessus.

Profits : Profits de 255 000 USD pour la société Broco et perte de 600 000 USD pour les victimes.

Moyens : Mots de passe et *login* volés. Les moyens techniques ne sont pas divulgués.

[146] Preuve d'amateurisme s'il en est.
[147] Voir bibliographie [85].
[148] Voir bibliographie [86].
[149] Voir bibliographie [87].

4.1.2. Vol de données personnelles et diffusion de fausse information

Cas: **Shalon "*Securities fraud on cyber steroids*"**[150]
Résumé: Ce cas a été appelé l'un des plus grands cybercrimes de l'histoire de par l'ampleur de la fraude. Plus de 100 millions de données personnelles dérobées provenant de 12 institutions financières dont 80 millions de données pour la seule banque JP Morgan. Un réseau international de criminels avec plus de 30 faux passeports de 17 nationalités différentes, qui ont profité du vol des données personnelles pour indument solliciter les futures victimes en les entraînant dans des escroqueries aussi variées que des schémas manipulatoires boursiers classiques comme du « *pump&dump* », des casinos internet illégaux et même une bourse d'échange illégale de *bitcoins*.
À l'aide d'au moins une vingtaine de sites internet promotionnels et d'une vaste liste d'adresses *emails* (auparavant ayant fait l'objet d'un vol relativement ciblé de clients d'institutions financières), les cybercriminels ont lancé des campagnes promotionnelles sur une dizaine d'actions pendant les années 2011 et 2012 en envoyant des *emails* semblant provenir de nombreuses sources apparemment différentes qui enjoignaient les investisseurs particuliers à investir dans ces actions, tout en se gardant bien de signaler qu'ils avaient auparavant investi eux-mêmes dans ces dernières. Une fois l'engouement autour de ces actions créé , les criminels les revendaient rapidement générant un confortable profit.
Profits: Plus de 100 millions d'USD au total dont au moins 2,8 millions d'USD pour la fraude boursière.

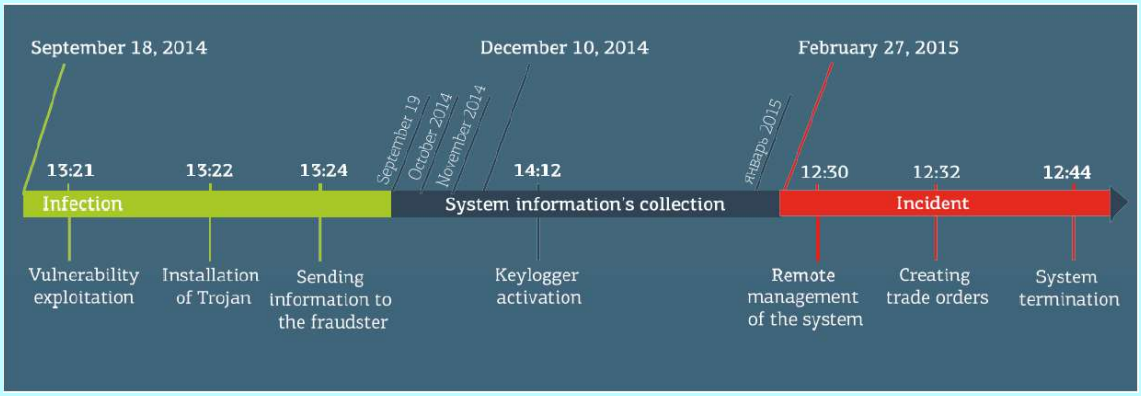
Cet exemple d'un groupe, dont le *business model* semble entièrement axé sur le « cyber », démontre à nouveau l'intérêt des groupes cybercriminels organisés pour la cybercriminalité boursière. Il montre également le danger, déjà mentionné précédemment, des pertes ou des vols de données personnelles, lesquelles peuvent être exploitées de multiples façons, ici avec de la promotion malveillante mais ciblée à des fins de manipulation boursière.

4.1.3. Intrusion de comptes de trading professionnels

Cas: **ENERGOBANK/CORKOW**[151]
Résumé: En février 2015, une cyberattaque contre des systèmes de *trading* d'une banque russe a pris place avec des transactions non autorisées pour un montant notionnel avoisinant les 500 millions d'USD[152] sur la devise Dollar/Rouble, pendant 14 minutes, grâce à un *malware* de type Trojan. Ces transactions ont fortement déstabilisé le cours de la devise normalement stable à 60/62 roubles pour un dollar pour évoluer vers 55 puis 66 roubles pour un dollar l'espace de quelques instants, avant de retrouver ses valeurs usuelles. Le résultat de cette attaque a été une perte réputationnelle importante pour cette banque, et certains experts estiment qu'elle n'était qu'un test préparatoire des cybercriminels pour une opération de plus grande envergure.
Profits : La banque a déclaré des pertes de 3,2 millions d'USD. Néanmoins, il faut remarquer que le cours de change a varié de presque 15 % de 66 à 55 roubles pour un dollar. Et que ce cours fixe aussi le prix de tous les instruments dérivés sur ce sous-jacent comme les CFDs ou autres. Il n'est donc pas impossible d'imaginer que des complices aient pu profiter de cette variation sur un autre marché.
Moyens : Pour mener leur attaque, les criminels ont utilisé le *malware* Corkow, aussi connu sous le nom de Metel, qui contient des modules spécifiques aux systèmes de trading russes[153]. Corkow permet ainsi

[150] Voir bibliographie [93], [94] et [95].
[151] Voir bibliographie [88] et [89].
[152] Néanmoins, seulement 250 millions ont fini par être exécutés.
[153] Comme QUIK de ARQA Technologies (https://arqatech.com/en/products/quik/) et TRANSAQ de ZAO. (http://www.transaq.ru/en/).

un accès à distance à ces derniers. Le 18 septembre 2014[154], les cybercriminels sont rentrés dans le système par l'exploitation d'une vulnérabilité et ont installé le Trojan qui se mettait régulièrement à jour pour éviter la détection par l'antivirus de la banque qui était pourtant fonctionnel. Group-IB avance même qu'en mars 2015, aucun antivirus n'était capable de détecter la version v.7.118.1.1 de Corkow. La phase de collecte d'informations a alors commencé et des « *keyloggers* » ont été activés en décembre 2014. Enfin le 27 février 2015, un accès à distance a été obtenu et les ordres de *trading* ont pu être émis. Enfin 14 minutes après l'envoi du premier ordre, les cybercriminels ont essayé d'effacer Corkow du système de *trading* ainsi que toute trace de son activité passée. Pour une analyse technique plus détaillée du malware Corkow voir *supra*.



4.1.4. <u>Des groupes cybercriminels organisés et sophistiqués</u>

Le cas ENERGOBANK est très instructif pour deux raisons :

- la cybercriminalité boursière attire des groupes cybercriminels organisés et hautement sophistiqués ;
- les attaques peuvent dorénavant atteindre les systèmes de *trading* des professionnels des marchés financiers et non plus seulement des particuliers, démultipliant les impacts sur l'intégrité des marchés.

Comme le révèlent les cas ENERGOBANK ou SWIFT (*cf. supra*), la sophistication des groupes cybercriminels spécialisés dans la finance/ la bourse est d'ailleurs remarquable, car elle allie une expertise informatique de très haut niveau[155] à une connaissance aigue des mécanismes financiers.

Si la cartographie des groupes cybercriminels spécialisés dans la finance n'est pas l'objet de cet ouvrage, on peut tout de même citer les acteurs reconnus suivants motivés par les gains économiques (contrairement aux hacktivistes), même s'il est délicat de les séparer si distinctement et de les considérer comme encore actifs ou non[156]: Corkow[157], Carbanak dont le cerveau a été arrêté tout récemment en

[154] Voir le graphique ci-dessous qui détaille les évènements suivants : exploitation de la vulnérabilité, installation du Trojan, envoi des informations au fraudeur, activation des keyloggers, contrôle à distance du système, création des ordres de trading, supression du système.

[155] Le directeur général de *Sophos,* Hagerman, fait observer que le volume et la variété des maliciels continuent de grandir. Une des tendances majeures réside dans la sophistication accrue des maliciels et des outils servant à les créer. Hagerman déclare également qu'un pourcentage grandissant de logiciels malveillants sont spécialement créés en fonction des cibles à atteindre. Ainsi, la sophistication ne serait pas nécessairement l'apanage exclusif des États, dans un contexte où les frontières entre cybercriminalité et cyberespionnage restent poreuses. Voir bibliographie [198].

[156] Voir bibliographie [199] et [200].

[157] Voir bibliographie [90].

Espagne début 2018[158], Cobalt[159], FIN4 (*cf. supra*), FIN7 dont trois membres ont également été arrêtés en Aout 2018[160], Lazarus[161] (alias Hidden Cobra, Dark Seoul, APT38)…

4.2. Prospectives

4.2.1. Intrusion de comptes de trading et applications mobiles

Il y a eu quelques exemples de piratages de comptes de *trading* de particuliers au Royaume-Uni et en France en 2011 et 2016 avec des modes opératoires très similaires à ceux qui sont présentés ci-dessus, mais les enjeux n'ont pas été trop importants jusqu'à présent et les intrusions vite détectées.

En revanche, d'après les autorités locales hongkongaises[162], la compromission des comptes de *trading* de particuliers à des fins de manipulation de cours des actions, semble être un problème particulièrement important, notamment à cause du nombre de *penny stocks* cotés, de la proximité des hackers chinois et de la faiblesse de la cybersécurité des courtiers par rapport aux autres acteurs financiers et aux banques de détail. Au moins sept courtiers et huit banques dont *HSBC Holdings Plc* and *Bank of China International (BOCI) Securities*[163] ont été la cible de telles attaques. Le phénomène a gagné en importance ces dernières années avec un triplement des cas en 2016 (81) par rapport à 2015.

En réaction, la SFC a ainsi proposé, dès le 13 octobre 2016[164], une revue de la cybersécurité des systèmes de *trading* mobiles et/ou par Internet. Après avoir rendu publique la consultation effectuée auprès du secteur en mai 2017[165], le 27 octobre 2017[166], de nouvelles *guidelines* ont été émises, proposant entre autres, une authentification à double facteur au vu de la pauvre sécurité apportée par les mots de passe. Au vu de l'évolution des habitudes et des technologies, toujours très rapide en Asie, le régulateur hongkongais a même dû émettre des *guidelines*[167] relatives au *trading* sur les messageries instantanées, encore plus sujettes aux cyberfraudes que les autres modes de communication. De manière générale, la région Asie-Pacifique[168], de par sa digitalisation extrêmement rapide, qui ne va pas nécessairement de pair avec un investissement corrélé dans la cybersécurité, notamment pour les petites et moyennes entreprises, très représentées dans le tissu économique régional et qui peuvent être des sous-traitants

[158] « Les hackers du groupe Carbanak ont débuté leurs méfaits fin 2013 avec leur logiciel Anunak qui ciblait les transferts financiers et les réseaux ATM (pour *Asychronous Transfer Mode*) des institutions financières. L'année suivante, ils sortaient une version plus sophistiquée d'Anunak, connue sous le nom de Carbanak, utilisée jusqu'en 2016. Puis, ils ont lancé une vague de cyberattaques encore plus sophistiquées avec le logiciel Cobalt Strike qui leur permettait d'ordonner aux guichets automatiques de « sortir » de l'argent à des moments déterminés à l'avance ». Voir bibliographie [201] et [202].
[159] Dans leur blog (voir bibliographie [91]), les auteurs soulignent que le groupe Cobalt a principalement pour cibles les banques mais aussi toutes les institutions financières et qu'il pourrait se montrer particulièrement intéressé par les bourses, comme prédit par le FinCERT de la banque centrale russe. Ce groupe Cobalt semble toujours extrêmement actif. (source : voir bibliographie [92]).
[160] Voir bibliographie [42].
[161] D'après cet article du 1er avril 2019 (voir bibliographie [203]), la société chinoise 360 Security a publié un rapport sur les activités du groupe de menace persistante et avancée (APT) Lazarus (alias Hidden Cobra, Dark Seoul, APT38) relatives aux plateformes de cryptomonnaie. Les détournements de fonds se seraient ainsi multipliés, notamment avec la dernière compromission en date de la plateforme DragonEX en mars 2019. En analysant cette attaque, les chercheurs ont identifié un faux logiciel de *trading* nommé Worldbit-bot utilisé par les attaquants, contenant un code malveillant, qui a été distribué au personnel interne des plateformes d'échanges de cryptomonnaie, sous prétexte de proposer une promotion sur ledit logiciel. Une porte dérobée a ainsi pu être installée sur les machines, permettant aux attaquants d'obtenir la clé privée du portefeuille et d'opérer sur les réseaux compromis pendant des mois.
[162] Voir bibliographie [96].
[163] Voir bibliographie [97].
[164] Voir bibliographie [98].
[165] Voir bibliographie [99].
[166]Voir bibliographie [100].
[167] Voir bibliographie [101].
[168] Voir bibliographie [102].

pour des entreprises plus grandes et plus internationales[169] , présente une cible de choix pour les cybercriminels.

La problématique de la sécurisation des applications et des comptes de *trading* semble être en réalité un problème beaucoup plus important que prévu, puisqu'une étude de juillet 2018[170] a montré que de nombreuses applications de *trading* (mobiles et de bureau), même parmi des acteurs américains aussi renommés que *Charles Schwab*, *Fidelity*, *Interactive Brokers*, *TradeStation*, étaient beaucoup moins sécurisées que leurs homologues de paiement bancaire. Certaines applications étaient même si peu sécurisées que les données envoyées au serveur n'étaient pas chiffrées, permettant ainsi des attaques comme celles de « l'homme du milieu » (« *Man-In-The-Middle* »). Néanmoins, le chercheur souligne que les plateformes opérées par Bloomberg et Capital One sont les plus sécurisées.

4.2.2. Les algorithmes

Les algorithmes sont au cœur des échanges financiers modernes. Suivant les classes d'actifs considérées, ils étaient déjà responsables sur la période 2014-2016 d'au moins 50 % à 80 % des échanges quotidiens des contrats futures sur la bourse d'échange américaine du CME (voir graphique ci-dessous), tandis que sur les marchés d'actions américains, le *trading* haute fréquence, qui est une sous-famille du *trading* algorithmique, représente au moins 50 % des échanges quotidiens depuis une dizaine d'années. Si on considère les ordres émis mais non exécutés, alors la présence du *trading* haute fréquence augmente à plus de 90 %.

Rappelons-nous l'achat malencontreux, en l'espace d'une demi-heure, de plusieurs milliards d'USD d'actions américaines par *Knight Capital*, société spécialisée dans le *trading* à haute fréquence, suite à une erreur informatique dans un de ses algorithmes (vraisemblablement un nouvel algorithme lancé en production[171]) et qui lui a coûté plus de 440 millions d'USD entraînant sa fusion ultérieure avec *Getco*, maintenant *Virtu Financial*.

[172]

[169] Rappelons nous de Target dont l'intrusion avait pu être réalisée grâce à son sous-traitant en charge du chauffage, de l'aération et de la ventilation (source : voir bibliographie [103]).
[170] Voir bibliographie [104].
[171] Voir bibliographie [106].
[172] Voir bibliographie [105]. Sur ce graphique, on distingue de haut en bas : les monnaies du groupe G10, les indices actions US, les taux des bons du Trésor américain, le pétrole, les métaux précieux, céréales et oléagineux.

Comment ne pas imaginer, dès lors qu'un cybercriminel, certes doué, ne puisse sciemment compromettre les algorithmes d'une telle société de *trading* pour manipuler le cours de certains instruments à des fins économiques ou simplement pour déstabiliser la bourse en envoyant des ordres de vente massifs en série ?[173]

Au vu de cette forte présence des sociétés de *trading* à haute fréquence dont les profits dépendent de leur rapidité (l'unité temporelle de référence est devenue la microseconde), et d'un point de vue conceptuel, il est intéressant de mentionner cette manipulation théorique[174] qui consisterait à les ralentir en injectant des données superflues en grand nombre dans les canaux de transmission reliant ces sociétés à la bourse. Cette attaque serait l'équivalent pour les algorithmes à haute fréquence d'une attaque en déni de service (DoS) pour les sites internet.

Enfin, de manière plus générale, on peut très bien imaginer une attaque par *malware* essayant de modifier le contenu des ordres d'un ou des participants, une fois arrivés à la bourse.

[173] Cette hypothèse n'est pas si irréaliste que ça puisque même la DARPA y travaille dans son projet « *Financial Markets Vulnerabilities Project* » (source : voir bibliographie [107]).
[174] Voir bibliographie [108].

5. Les cyberdiffusions de fausse information

Si la diffusion de fausse information est une technique de manipulation boursière vieille comme le monde, que l'on songe à l'annonce de la fausse mort de Napoléon orchestrée en février 1814 au *London Stock Exchange* afin de faire augmenter les bons du Trésor anglais[175], nul ne peut contester, et ce d'autant plus avec tous les débats actuels autour des « *fake news* »[176] et des nouvelles lois ad-hoc[177], qu'à l'ère numérique, avec les sites Internet, les réseaux sociaux et les courriels, la diffusion de fausse information est devenue beaucoup plus facile, plus rapide, et avec une portée beaucoup plus large ; donc avec un impact sur les marchés financiers, dopés à l'information instantanée[178] et aux rumeurs, beaucoup plus important. Par exemple, le 27 juin 2017[179], une fausse nouvelle constituée d'une simple photo d'un *crash* d'hélicoptère accompagnée de quelques mots sur la mort de Vitalik Buterin, le créateur de l'Ethereum, avait suffi pour faire perdre 4 milliards d'USD de valeur à cette cryptomonnnaie en une seule journée. De même, le 22 novembre 2016, un faux communiqué de presse de Vinci alléguant de la découverte de fraudes comptables faisait plonger le cours de cette dernière de près de 19 % en 7 minutes, soit une perte momentanée de capitalisation d'environ 7 milliards d'euros.

Les motivations des diffusions de fausses informations sont souvent économiques[180] (le criminel cherche à tirer un profit économique personnel de l'opération), mais elles peuvent être aussi activistes[181], vu la symbolique idéale et l'impact potentiellement important sur la valorisation des sociétés visées. Sans aucun doute, du sabotage économique de la part d'un concurrent ou de la déstabilisation étatique peuvent aussi être envisagées.

La diffusion de fausse information peut, comme les cybermanquements d'initié, toucher tous les intervenants de la chaîne de diffusion d'information du monde boursier. Ainsi les diffuseurs d'informations financières spécialisés (comme Bloomberg ou Reuters) sont naturellement souvent les premiers visés.. D'influentes agences de notation ont également pu, par le passé, et sans aucune manipulation, diffuser des fausses informations. Les sources de « désinformation » financière sont nombreuses et il est évident que la désinformation trouve des alliés plus qu'efficaces avec les réseaux sociaux, notamment Twitter.

[175] Voir bibliographie [109].
[176] Dernier article en date montrant l'ampleur du phénomène : voir bibliographie [110].
[177] Voir bibliographie [111].
[178] Grâce au trading algorithmique à haute fréquence et à l'automatisation de la lecture des nouvelles financières.
[179] Voir bibliographie [112].
[180] Il ne semble pas que, dans le domaine particulier de la cybercriminalité boursière, les motivations des attaquants soient fondamentalement différentes de celles de la cybercriminalité classique oùles trois quarts des attaques sont motivées par un profit économique (source : https://www.hackmageddon.com)
[181] On reviendra à sur cet aspect dans l'analyse des cas. Un exemple d'activistes fameux est celui des « Yes Men », aux Etats-Unis. C'est une organisation activiste environnementale spécialisée dans la production de fausses nouvelles qui a ciblé des multinationales, en particulier pétrolières. En 2010, le géant américain Chevron a été victime d'un canular très sophistiqué, avec une campagne publicitaire détournée et faisant croire qu'il endossait la responsabilité de plusieurs catastrophes environnementales. En 2011, c'était au tour du conglomérat industriel américain GE, accusé à l'époque de bénéficier de faveurs fiscales indues, d'être visé par un faux communiqué des Yes Men, annonçant qu'il allait restituer 3,2 milliards de dollars au fisc. Ces derniers étaient allés jusqu'à organiser une fausse conférence de presse à Washington, en se faisant passer pour des représentants de la Chambre de commerce, jusqu'à ce qu'un membre de la vraie Chambre débarque et dévoile le pot-aux-roses.

5.1. Les cas

5.1.1. La galaxie Vinci

Cas: Emulex: « *Mother of all hack*"[182]

Résumé : Le 24 août 2000, la société Emulex cotée au NASDAQ spécialisée dans la fibre optique, voyait son action chuter de 113 à 43 dollars, en seulement dix-huit minutes, soit une baisse de 60 % de la valorisation de l'entreprise consécutive à la diffusion d'un faux communiqué de presse diffusé sur *Internet Wire* (un diffuseur d'informations financières), faisant état de la démission de son président, de l'ouverture d'une enquête par la SEC et de la révision de son chiffre d'affaires à la baisse. Ce faux communiqué avait en fait été rédigé par un jeune étudiant de 23 ans dénommé Mark Jakob, qui avait travaillé chez *Internet Wire* pour le service d'information boursière en ligne. Fin connaisseur des processus internes, Jakob téléphone au bon interlocuteur pour annoncer l'arrivée imminente de la dépêche de presse et l'expédie par courrier électronique à *Internet Wire*, à partir d'un ordinateur en libre accès dans la bibliothèque de son ancienne université. Le bon protocole ayant été respecté, *Internet Wire* ne se soucie pas de vérifier le contenu de la dépêche. Celle-ci est publiée le 24 août 2000, et très vite reprise par plusieurs services de presse, tels Bloomberg et Dow Jones[183]. La réaction est immédiate, le cours de l'action chute rapidement. Jakob effectue alors des achats d'actions au plus bas sur Internet à partir d'une chambre d'hôtel à Las Vegas lui permettant à la fois de déboucler sa position courte de 3 000 titres prise au préalable, le 17 et 18 août 2000, et de reprendre une nouvelle position longue de 3 500 titres qu'il débouclera avec profit, le 28 août 2000, une fois la fausse information démentie et le cours de l'action remonté…En parallèle de ces actions de relations publiques visant à démentir les fausses informations, la société dépose plainte et fait intervenir le FBI, ainsi que la SEC. L'enquête permettra l'arrestation du présumé coupable le 31 août.

Profits : Perte momentanée de capitalisation boursière de l'ordre de 2,5 milliards d'USD. Le profit généré pour le criminel est en revanche seulement de 241 000 USD.

Cas: Whitehaven Coal[184]

Résumé : Le 7 janvier 2013, un faux communiqué émanant apparemment de la banque ANZ annonçait que cette dernière avait annulé un prêt de 1,2 milliards d'USD accordé à la société minière australienne Whitehaven Coal dans le cadre du projet Maules Creek pour plusieurs raisons économiques mais aussi environnementales. Le cours de l'action de la société minière chuta alors de 9 % à 3,21 USD en l'espace de quelques instants avant que l'action ne soit suspendue. Un groupe activiste écologique du nom de « *Front Line Action on Coal* » revendiqua l'action. L'instigateur principal Jonathan Moylan (26 ans) plaida coupable et a été condamné à 1 an et 8 mois de prison mais relâché immédiatement sous réserve de bonne conduite et d'une amende de 1000 USD[185].

[182] Voir bibliographie [113].

[183] Parallèlement, une Action Class était intentée par les épargnants lésés contre Internet-Wire et Bloomberg, sociétés spécialisées dans la diffusion de communiqués financiers, prétendant que lesdites sociétés avaient involontairement diffusé de fausses informations. Il était reproché à ces deux sociétés d'avoir violé les règles de contrôle interne pour n'avoir pas vérifié l'exactitude et l'authenticité du communiqué de presse Emulex avant sa publication. Selon la plainte, Internet-Wire a reçu le communiqué l'après-midi du 24 août alors que le 25 au matin coïncide avec l'ouverture des marchés. Durant cette période sensible, le média aurait dû approfondir l'examen de l'information. Enfin, la société Emulex utilisait traditionnellement le magazine Business Wire et non Internet Wire, pour diffuser ses communiqués, cette modification dans le support de diffusion devait conduire à plus de prudence dans l'étude des informations transmises. À la suite de cette affaire, la vérification de l'authenticité des communiqués diffusés par des professionnels devait être renforcée.

[184]Voir bibliographie [114].

[185] Voir bibliographie [204].

Profits/Impact : Baisse momentanée de la capitalisation boursière de 315 millions d'USD. Néanmoins, un article de presse estime la perte « réelle » pour les actionnaires à seulement 450 360 USD[186] (voir la discussion *infra* qui estime en général le préjudice réel entre 1/1000 et 1/100 de la perte de capitalisation).

Cas: Fingerprints cards[187]

Résumé : Le 11 octobre 2013, un faux communiqué a été diffusé et annonçait l'acquisition de la société suédoise *Fingerprints cards*, spécialisée dans la reconnaissance digitale, par *Samsung* pour 650 millions d'USD. Ce communiqué, bien que faux, fut même repris sur le site officiel de *Fingerprints cards*…Le cours de l'action s'envola de près de 50 % en l'espace de dix minutes avant d'être suspendu. Les faits ont été dénoncés à la police et au régulateur boursier suédois. Les résultats de l'enquête ne sont pas connus.

Profits/Impact : Hausse momentanée de la capitalisation boursière de 200 millions d'USD.

Cas : G4S[188]

Résumé : Le 12 novembre 2014, G4S, une société de sécurité notamment chargée de la surveillance des camps de migrants d'une capitalisation boursière de 3 638 millions de GBP, a été la victime d'un faux communiqué qui annonçait une révision comptable ainsi que le licenciement de son directeur financier. Le cours du titre G4S a subi un faible impact (-0,94 % pour finir par un gain de 2 % en fin de journée) par la diffusion de ce faux communiqué, car même s'il a pu tromper certains journalistes et provoquer de nombreux tweets, il n'a pas été repris par Bloomberg. Une revendication par des activistes politiques contre les politiques répressives anti-migrants a également été diffusée après le faux communiqué.

Profit/Impact : Baisse momentanée de plus de 40 millions de GBP de capitalisation boursière mais relativement insignifiante par rapport à la volatilité du titre. Pas de gain criminel à notre connaissance. Il ne semble pas qu'une enquête ait été diligentée par les autorités ou qu'elle ait abouti.

Moyens : Le faux *mail* utilisait un nom de domaine qui avait été enregistré une douzaine de jours auparavant sous une fausse identité hollandaise et qui ressemblait fortement à l'adresse officielle de G4S. De plus, le *hoax* semblait quelque peu grossier avec des fautes d'orthographe et des mots manquants, mais surtout il n'était pas repris par le *London Stock Exchange's Regulatory Information Service* (RNS) qui doit concentrer toutes les annonces officielles des sociétés qui y sont cotées. Beaucoup plus intéressant est le fait que, dans certaines revendications relatives au cas G4S effectuées sur des sites alternatifs comme *Indymedia*, les auteurs aient conseillé l'utilisation d'un guide intitulé « *Prank the pranksters ! Playing around with information and fakes in the age of immaterial capitalism*" [189]

Cas: Immunovaccine[190]

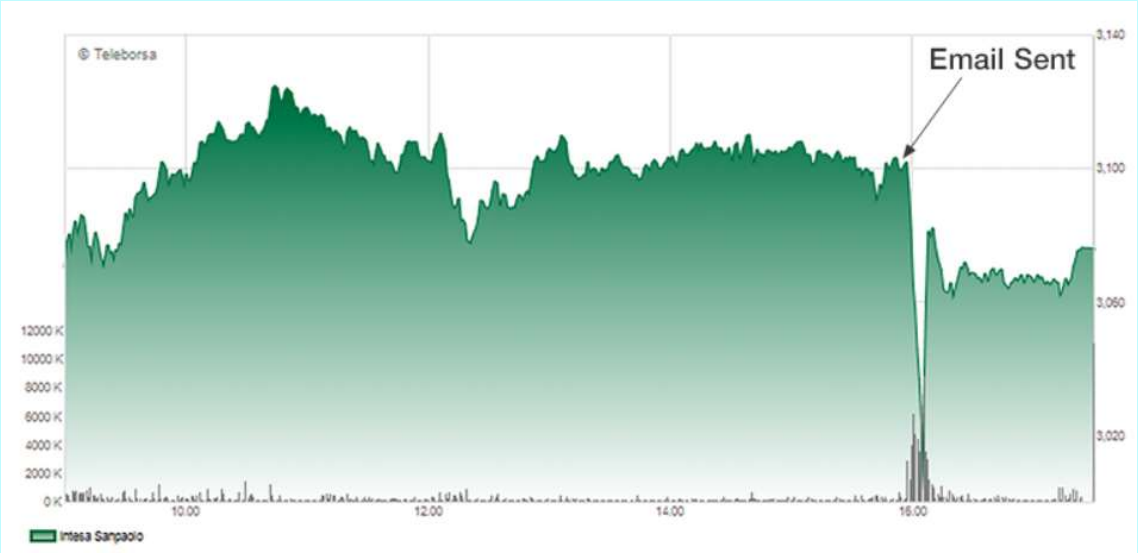
Résumé : Le 3 mars 2015, un faux communiqué annonçait un partenariat de grande ampleur entre la société pharmaceutique canadienne *Immunovaccine* et la société *Gilead Sciences*. Le cours de l'action *Immunovaccine* bondit de 24 % et cette dernière fut suspendue.

Profits/Impact : Le régulateur boursier canadien (IIROC) annonça qu'il allait annuler les transactions réalisées pendant le *hoax* ou modifier le prix de ces dernières à sa valeur initiale.

[186] Voir bibliographie [205].
[187] Voir bibliographie [206] et [207].
[188] Voir bibliographie [115].
[189] Voir bibliographie [116].
[190] Voir bibliographie [208] et [209]

Cas : Banca Intesa[191]

Résumé : Le 24 avril 2015, *Banca Intesa San Paolo*, l'une des plus grandes banques italiennes, a été la victime d'un faux communiqué qui annonçait des manipulations comptables ayant un impact de 2 milliards d'EUR sur ses résultats ainsi que le licenciement de son président directeur général, Carlo Messina. Le cours du titre a été fortement impacté avec une baisse de 4 % en 8 minutes à 2,99 EUR avant de rebondir rapidement à ses niveaux antérieurs[192]. L'opération a été revendiquée, sur un site alternatif *Indymedia Piemont*, par le groupe activiste écologique « *No Tav* » qui lutte contre le projet de train à grande vitesse Lyon-Turin dont la banque *Banca Intesa* est une des contributrices .



Profit/Impact : Baisse momentanée de 2 milliards d'EUR de capitalisation boursière. À notre connaissance, l'enquête est toujours en cours.

Moyens : Le faux *mail* utilisait un nom de domaine intesasanpaolo-group.com qui avait été enregistré trois semaines auparavant sous une fausse identité italienne et qui ressemblait fortement à l'adresse officielle intesasanpaolo.com. Le faux mail renvoyait à un site miroir en tout point identique au site officiel de *Banca Intesa* sauf pour la partie faux-communiqué. Les cybercriminels ont pris même la peine de répondre aux emails des journalistes en signant du nom du véritable responsable des relations medias du groupe. Le '*hoax* n'était donc pas grossier et le *modus operandi* très proche des cas G4S et Vinci.

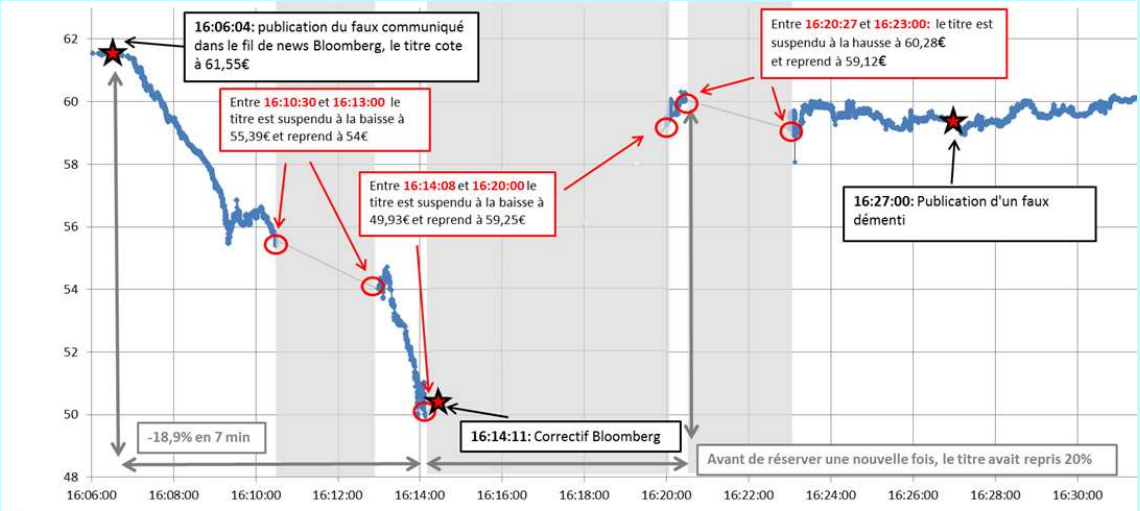
Cas: Rachat de Twitter[193]

Résumé : Le 14 juillet 2015, un faux article émanant apparemment de Bloomberg annonçait une offre d'achat sur Twitter pour 31 milliards d'USD (contre 25 milliards d'USD pour la valorisation de la veille). L'information contenue dans l'article était ensuite relayée par un présentateur vedette de CNBC par un *tweet*, [194]. Le cours de l'action Twitter s'envolait alors de 8 % en l'espace de dix minutes. Notons aussi que, derrière chaque rumeur, peut se cacher une once de vérité et que dans le cas de Twitter, des rumeurs insistantes sur la mauvaise santé de cette dernière et son éventuel rachat circulaient déjà. Le démenti rapide de Bloomberg suffit à faire retomber le cours à ses niveaux antérieurs, en moins de 5 minutes.

[191] Voir bibliographie [117], [118] et [119].
[192] Voir le graphique ci-dessous où « email sent » fait référence à l'envoi initial du faux communiqué par courriel.
[193] Voir bibliographie [120].
[194] Ce seul *tweet* ne peut être mis en cause et il est évident que les *webcrawlers* ont eu leur rôle à jouer dans la propagation de cette nouvelle.

Profits/Impact : Augmentation de la capitalisation boursière de 2 milliards d'USD. *A priori*, pas de profit personnel criminel. L'enquête semble toujours en cours.
Moyens : Un faux site Internet *Bloomberg.market*, copiant point par point le vrai site *Bloomberg.com*, avait été enregistré quatre jours auparavant. Le nom du rédacteur de l'article était celui d'un vrai journaliste de Bloomberg.

Cas : VINCI[195]
Résumé : Le 22 novembre 2016, Vinci est victime d'un faux communiqué de presse officiel annonçant la découverte d'erreurs comptables pour un montant de 3,5 milliards d'EUR et le licenciement du directeur financier responsable. Plus précisément, à 16h05, le faux communiqué est envoyé par *mail* à plusieurs rédactions de presse spécialisée. Dès 16h07, l'information est diffusée par l'agence Bloomberg, le cours chute alors de presque 19 % en l'espace de 7 minutes, soit un milliard d'EUR de capitalisation boursière par minute. Le démenti de Bloomberg à 16h14 :11 permettra au titre de recouvrer quasiment toute sa valeur aussi vite qu'il l'avait perdue. A 16h27, un faux démenti des criminels, , rajoutera la confusion dans certaines salles de rédaction mais sans trop d'impact sur le cours déjà stabilisé. Enfin à 17h35, un dernier faux communiqué de pseudo-revendication activiste[196] sera envoyé par mail.



Profit/Impact : Baisse momentanée de plus de 7 milliards d'EUR de capitalisation boursière… Les pertes réalisées pourraient être plus faibles (cf. discussion *infra*).
Moyens : Le faux *mail* utilisait un nom de domaine vinci.group qui avait été enregistré plusieurs jours auparavant sous une fausse identité hollandaise et qui ressemblait fortement à l'adresse officielle vinci.com. Le faux mail renvoyait à un site miroir en tout point identique au site officiel de Vinci sauf pour la partie faux-communiqué et le communiqué fournissait le vrai nom du responsable des relations presse mais avec un faux numéro, au bout duquel l'usurpateur a répondu à quelques appels de journalistes. Le *hoax* n'était donc pas grossier. Le *modus operandi* est très proche des cas G4S et Banca Intesa.

Cas: Fausse lettre du CEO de BlackRock[197]
Résumé : Le 16 janvier 2019, à quelques jours de la parution officielle de la lettre annuelle du CEO de la célèbre société de gestion américaine *BlackRock*, Larry Finck, un faux courriel usurpant l'identité de ce

[195] Voir bibliographie [121] et [122].
[196] Dont la plupart des acteurs s'interrogent sur l'authenticité au vu de son style et de son contenu.
[197] Voir bibliographie [210]

dernier avec l'adresse « larry.finck@blackrock-esg.com » renvoyant vers un faux site Internet lequel reprenait les codes du site officiel de BlackRock, a été envoyé à plusieurs médiass. Cette lettre mentionnait un virage environnemental et écologique pour BlackRock et un désinvestissement des entreprises ne respectant pas les accords de Paris. Le jour même, à 14h31, BlackRock démentait ces informations dans un tweet publié sur son compte officiel. Aucun impact sur les cours boursiers *a priori* pour cette désinformation aux accents activistes prononcés n'a été constaté.

Il faut noter que devant cette cybercriminalité, nécessitant peu de moyens et facilement anonyme, les enquêteurs ont souvent plus de chances d'aboutir s'il suivent les traces laissées par les transactions boursières du cybercriminel, (). Il existe en effet sur Internet de nombreuses ressources en libre accès permettant au cybercriminel novice de se perfectionner dans la fabrication de son *hoax* boursier[198]. Il est ensuite très facile pour le fraudeur de rester anonyme sur Internet, soit par l'utilisation d'un Wifi public, soit par l'utilisation de VPN[199] ou du réseau TOR[200], et ce d'autant plus que les contrôles d'identité demandés lors de l'enregistrement de nom de domaine ou de l'hébergement de site Internet sont quasiment inexistants et que la durée de conservation des données est faible. L'utilisation de moyens de paiement comme les cartes prépayées ou les cryptomonnaies permet enfin de payer ces services sans rompre son anonymat[201]. Les enquêtes étant souvent internationales, la coopération entre les différents régulateurs nationaux est ici primordiale mais en pratique, l'hétérogénéité des pouvoirs de ces derniers face à des entités souvent non régulées et la relative lenteur des transmissions, sont des freins puissants à l'exploitation des preuves numériques. Pour le cybercriminel, l'investissement et les risques sont donc plutôt faibles mais l'impact est potentiellement très important, puisque pouvant s'élever à plusieurs centaines de millions voire des milliards d'EUR de capitalisation boursière *momentanément* perdue. Les coupe-circuits mis en place dans les bourses permettent néanmoins de stopper une chute trop importante.

Dans « *Les 3F du HoaxCrash: fausse donnée, flash crash et fort profit* », les auteurs, après avoir présenté en détail le cas Vinci de 2016, et rapidement d'autres cas similaires définissent trois paramètres intéressants : la durée de validité d'un *hoax* avant publication d'un démenti, l'efficacité du *hoax* comme le ratio du gain réalisé par l'attaquant sur la complexité (de Kolmogorov[202]) du mode opératoire et la puissance d'un hoax comme le ratio de la variation totale du cours sur cette même complexité. Enfin, au vu de la rapidité des évènements, ils proposent, sans préciser sa nature exacte, le développement d'un

[198] Au moins un document est disponible « Prankthepraksterpdf », véritable manifeste et bible contenant tout le monde opératoire ainsi que toutes les étapes et astuces pour réussir son *hoax* boursier : pourquoi et comment élaborer et diffuser un faux communiqué de presse financier, obtenir les *emails* des journalistes, créer des faux sites, envoyer des *mails* d'une fausse adresse en exploitant les faiblesses du protocole SMTP avec Telnet sans oublier de rester anonyme…

[199] VPN pour « Virtual Private Network ». C'est un réseau privé « virtuel » qui permet de créer un lien direct et sécurisé entre deux ordinateurs distants. Des sociétés proposent donc des services VPN en établissant un VPN entre votre ordinateur et un serveur de cette société. Lors de la connexion à l'Internet sur votre ordinateur, seule l'adresse IP de ce serveur sera visible. Bien entendu, les sociétés proposant des services de type VPN peuvent ou non enregistrer vos connexions et donc votre adresse IP d'origine.

[200] TOR pour « The Onion Router ». C'est un réseau informatique mondial et décentralisé dont les serveurs sont aussi appelés nœuds. Ce réseau permet d'anonymiser l'origine des connexions à Internet (la fameuse adresse IP d'origine) en faisant rebondir les échanges sur différents nœuds, qui ne connaissent que l'adresse IP du nœud précédant et suivant. TOR propose également à ses utilisateurs un ensemble de services cachés, en cachant l'identité du serveur qui les héberge. Ce serveur recevra une adresse en .onion et ne sera accessible qu'avec TOR. C'est une partie du fameux *Dark Web*.

[201] Même si certains paiements réalisés par *Bitcoins* peuvent être tracés, il ressort que les plateformes d'échange *bitcoins*/FIAT ne sont pas toutes exigeantes en termes de KYC « *Know Your Customer* ». La législation européenne est en train de changer à cet égard mais l'harmonisation mondiale est encore loin.

[202] La complexité de Kolmogorov, en théorie de l'information (ou complexité aléatoire ou complexité algorithmique) d'un objet (nombre, image numérique, chaîne de caractères) est la taille du plus petit algorithme (dans un certain langage de programmation fixé) qui engendre cet objet. Cette quantité peut être vue comme une évaluation d'une forme de complexité de l'objet. Source : Wikipedia.

réseau d'agents intelligents évaluant en temps réel la véracité des messages publiés afin d'éviter de nouveaux cas.

Si la définition de la puissance d'un *hoax* est essentielle, puisqu'une manipulation va souvent faire varier le cours du titre de manière importante et brutale sans que le criminel puisse en profiter pleinement (ou ne veuille en profiter dans le cas d'un activiste), on pourrait raffiner le concept. D'une part, en pondérant cette puissance par la volatilité habituelle du titre (car faire varier le cours de x % pour une action très volatile n'est pas la même chose que faire varier un cours de x % pour une action très stable), et d'autre part, par les prix et volumes des transactions effectivement réalisées sur le marché pendant la durée de validité de le 'hoax (car une seule action échangée au cours le plus bas n'est pas la même chose que 1 million d'actions échangées tant pour la « fiabilité » du prix que pour les potentielles victimes ayant vendu. Et ce d'autant plus que dans le cas d'un hoax, la valeur revient rapidement à son niveau d'origine).

Une rapide étude des ordres de grandeur tendrait à prouver que la perte effectivement réalisée par les actionnaires échangeant su la période hoax serait de 100 fois à 1000 fois plus petite que la perte de valorisation boursière « naïve »[203]. Nous ne nous attarderons pas sur ce sujet et considérerons seulement, dans l'étude de nos cas, le gain réalisé par le criminel et la variation quasi-instantanée de valorisation boursière, qui, même si critiquable pour les raisons susmentionnées, reste un indicateur évocateur, facile et robuste.

Enfin, il apparait évident à la lumière de tous ces cas au mode opératoire presque identique, que la question de la diffusion de l'information financière « officielle » est cruciale. Ces affaires montrent la nécessité de réfléchir avec l'ensemble des parties concernées (entreprises cotées, diffuseurs d'information, régulateur boursier[204], bourses[205]…) aux mesures susceptibles de prévenir la survenance de tels incidents ou d'en limiter les conséquences. À la suite de cet incident, l'AMF a par exemple défini, dans son communiqué de presse du 23 février 2017[206], des bonnes pratiques pour les émetteurs et les agences de presse, visant, d'une part, à clarifier le canal officiel de diffusion de l'information de l'émetteur pour mieux s'assurer de son authenticité et, d'autre part, à renforcer les procédures de sensibilisation et de cybersécurité des agences de presse pour éviter tout piratage en amont (réception d'un faux communiqué considéré comme vrai par les journalistes dans les cas ci-dessus), ou en aval (diffusion d'un faux communiqué directement dans les systèmes d'information de l'agences de presse ou du diffuseur).

---

[203] Le cas de Vinci est à cet égard éclairant et symbolique. 19 % de baisse (en moins de 10 minutes) correspond à 7 milliards de capitalisation. Néanmoins si on s'attache aux seules transactions réalisées pendant la période de baisse (un peu plus d'un million de titres vendus à des prix variant entre 61,5 euros et 50 euros), le préjudice approximatif subi par les victimes qui auraient donc vendu leurs actions Vinci à un prix inférieur (approximativement 55,75 euros soit la moyenne entre 61,5 euros et 50 euros) au prix « pré fausse annonce » de 61,5 euros serait seulement de 6 millions d'euros environ.
De manière générale, et en s'attachant à obtenir des ordres de grandeur seulement, un *hoax* entrainant une baisse de x% du cours en 10 minutes entrainera une reduction « naive » de capitalisation de x% mais en réalité aura un impact préjudiciable maximum sur les intervenants du marché (sans inclure les conséquences réputationnelles ou d'image) de seulement IPM=(x % prix/2)(10/480)(facteurvolumepanique)(Ndaily) où (x % prix/2) représente le manque à gagner par action en euros, (10/480)(Ndaily) représente la quantité moyenne de titres échangés en 10 minutes avec Ndaily le volume quotidien échangé et facteurvolumepanique représente l'effet multiplicateur du volume du à l'effet news/panique.
Si on remplace le prix de l'action par Capiglobale/Ntot avec Capiglobale la capitalisation boursière totale de la société, Ntot le nombre total d'actions de la société et en approximant (10/480)/2 par 1/100, on a encore IPM= (facteurvolumepanique)x % (1/100)(Capiglobale)(Ndaily/Ntot) soit encore en estimant que le volume moyen d'actions échangé quotidiennement Ndaily représente environ 1 % du nombre d'action total, IPM= x % (Capiglobale)(facteurvolumepanique)(1/10 000) soit presque 100 fois à 1000 fois (suivant que l'on prenne un facteurvolumepanique de 100 ou de 10) moins que l'estimation naïve relative à la variation de capitalisation .

[204] Voir infra les cas de diffusion de fausse information par le système de déclaration réglementaire EDGAR.

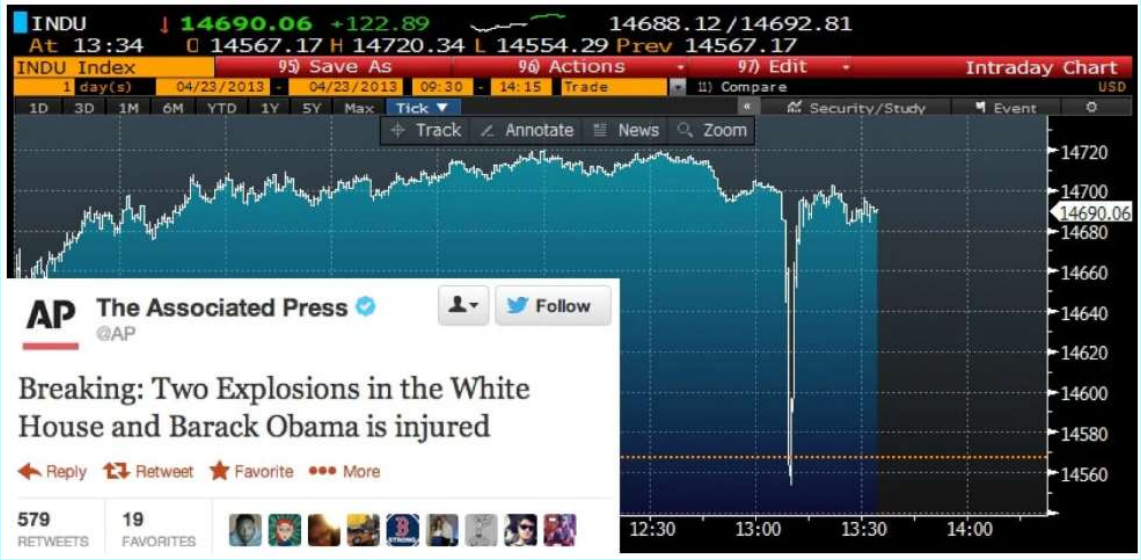
[205] Comme vu dans le cas G4S, certaines bourses disposent également d'un registre officiel concentrant les déclarations réglementaires ou les annonces des émetteurs.

[206] Voir bibliographie [123].

5.1.2. *Diffusion de fausse information par Twitter*

Cas: AP Tweet Obama[207]

Résumé : Le 23 avril 2013, le compte Twitter de l'Associated Press, suivi par deux millions de personnes, a été compromis et usurpé pour envoyer à 13h08 le message suivant : « *Breaking: Two Explosions in the White House and Barack Obama is injured* ». Les cours de nombreux instruments financiers ont instantanément chuté de 1 %, provoquant le chaos sur les marchés. Les démentis de l'AP et de la Maison Blanche ont immédiatement restauré le calme et les valorisations antérieures en moins de deux minutes.



Profits/Impact : Perte de valorisation boursière quasi instantanée, basée sur le S&P500, de 136,5 milliards d'USD ! La Syrian Electronic Army a revendiqué l'attaque mais les enquêtes menées par le FBI et la SEC semblent toujours en cours.

Cas : **Dissémination de faux tweets**[208]

Résumé : Le 29 janvier 2013, un trader écossais du nom de Craig envoyait une série de huit tweets en 90 minutes dans lesquels il écrivait que la société *Audience* faisait l'objet d'une enquête du DoJ (« *Department of Justice* »), à partir d'un compte enregistré par ses soins mais usurpant l'identité et les codes graphiques d'un analyste financier très reconnu « Muddy Waters ». Le cours de la société *Audience* a plongé de 28 %, entraînant une suspension à la baisse, avant de reprendre la cotation aux niveaux antérieurs une fois la supercherie dévoilée, notamment par le « vrai » Muddy Waters. Le lendemain, Craig a réitéré le procédé avec une autre société pharmaceutique *Sarepta Therapeutics* sous enquête de la FDA (« *Food&Drug Administration* ») et un autre compte usurpant l'identité d'un autre analyste (*Citron Research*). Aux mêmes causes correspondent les mêmes effets et le cours de Sarepta a plongé de 16 %.

Profits/Impact : Une centaine de dollars pour le cybercriminel (la faiblesse du gain semblant s'expliquer par le *timing* inapproprié des transactions). Néanmoins, les pertes (passagères) de valorisations pour les deux sociétés montent à environ 80 millions d'USD pour *Audience* et plus de 300 millions d'USD pour *Sarepta*.

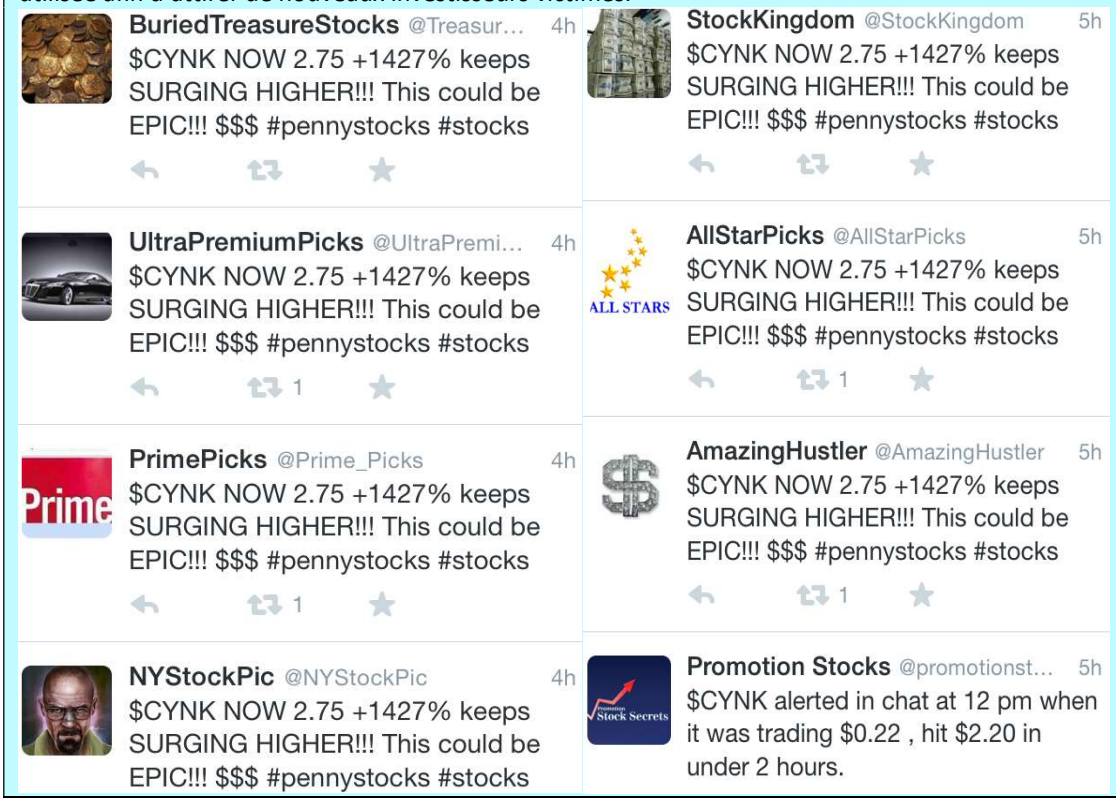
Cas : **CYNK**[209]

[207] Voir bibliographie [124 et [125].
[208] Voir bibliographie [126].
[209]Voir bibliographie [127], [128] et [129].

Résumé : Ce cas est l'un des cas de « *pump&dump* » les plus emblématiques, puisqu'une société dont les actifs ne dépassaient pas 1400 USD et qui n'avait jamais été cotée a, en l'espace d'un mois, du 17 juin au 10 juillet 2014, vu son cours exploser à près de 22 USD par titre, pour une capitalisation boursière de près de 4,5 milliards d'USD. Le 11 juillet, le titre a été suspendu par la SEC pour ne coter plus que 0,6 USD le 28 juillet lors de la réouverture. Le criminel, ici le fondateur de la société cachée derrière des prête-noms, a été inculpé par la SEC, en 2015.

Profits/Impact : La SEC a arrêté la cotation du titre avant que le criminel ne puisse en profiter en vendant ses actions. Mais des investisseurs particuliers ont été lésés. Hausse de la valorisation de près de 4,5 milliards d'USD.

Moyens : Une intense campagne promotionnelle utilisant les sites spécialisés et les médias sociaux a été utilisée afin d'attirer de nouveaux investisseurs victimes.



Twitter, comme l'ensemble des réseaux sociaux, est le terrain de jeu rêvé pour la diffusion de fausses informations : quasi-anonymat, rapidité et possibilité de toucher un large public notamment grâce à des faux comptes parfois robotisés (« *bots* ») et louables à la commande. En 2018[210], Facebook avait supprimé plus d'un quart de ses comptes car prétendument faux et, en 2017[211], une étude révélait qu'au moins 15 % des comptes Twitter pouvaient être des *bots*. Toutes les applications « réseaux sociaux » sont touchées, ainsi Whatsapp supprime-t-elle 2 millions de comptes par mois pour lutter contre les fausses informations[212].

Ces « *social bots* » semblent si capables d'influencer l'opinion que la DARPA (« *The Defense Advanced Research Projects Agency* ») s'en était émue, dès 2015, en consacrant son concours[213] à la détection de

[210] Voir bibliographie [130].
[211] Voir bibliographie [131].
[212] Voir bibliographie [211].
[213] Voir bibliographie [132].

ces robots influenceurs. Depuis, les dernières élections américaines avec l'éventuelle ingérence russe par ces mêmes robots sociaux lui ont donné raison et le sujet a pris de l'ampleur[214].

On ne détaillera pas les mécanismes à l'œuvre dans la diffusion de la désinformation sur les réseaux sociaux, même si certains résultats concernant la propagation supérieure du « faux » comparé au « vrai », peuvent laisser perplexes[215]. On soulignera néanmoins que ces techniques de diffusion de fausses informations servent évidemment les cybercriminels boursiers, comme dans les cas décrits ci-dessus, qui sont loin d'être isolés, puisque la SEC a émis des alertes spécifiques[216] visant à mettre en garde les investisseurs particuliers contre les rumeurs et recommandations qui proviennent des medias sociaux et qui peuvent servir à des manipulations de type « *pump&dump* ». Ainsi, dans l'article "*Market manipulation and suspicious stock recommendations on social media"*[217], T.Renault montre, en analysant plusieurs millions de messages envoyés sur Twitter relatifs aux actions à faible cotation, qu'une activité anormale est souvent associée à une large variation de prix le jour même et un déclin la semaine d'après. De plus, cette activité anormale semble être concentrée dans certains *clusters* de comptes Twitter, favorisant l'hypothèse de campagnes manipulatoires. Si les exemples se limitent jusque-là aux actions, il convient de noter que potentiellement toute la sphère financière peut-être concernée .

Enfin, on rappellera que l'automatisation couplée à la recherche à tout prix de la rapidité, la propension naturelle des acteurs de la finance à se tenir informés des rumeurs[218] et l'existence d'algorithmes spécifiques dont les ordres de *trading* sont directement dépendants du contenu circulant sur les media sociaux, que ce soit simplement de la lecture automatisée (sans intervention humaine) du contenu de comptes Twitter de sources officielles ou des signaux plus complexes basés sur l'analyse de l'activité même de Twitter (analyse des sentiments, des hashtags ou des comportements…) rend les marchés financiers encore plus susceptibles de succomber à ce type de manipulation.

5.1.3. Diffusion de fausse information par EDGAR

Cas: EDGAR IDTI[219]

Résumé : Le 12 Avril 2016, Aly, un résident pakistanais a acquis un large bloc d'options d'achat en dehors de la monnaie avec un délai d'expiration très court sur l'action *Integrated Device Technology, Inc.* ("IDTI"). Quelques instants après, Aly remplissait une fausse déclaration (Schedule 13D) sur le site EDGAR du régulateur boursier américain dans laquelle il annonçait détenir, avec un groupe d'investisseurs, plus de 5 % du capital d'IDTI et avoir fait une offre de rachat de la compagnie au comité exécutif avec un premium de 65 % par rapport au prix du marché. Suite à cette déclaration, rendue instantanément publique par le site EDGAR, le cours de l'action s'est envolé de 25 % en moins de 10 minutes et Aly a pu revendre ses options avec profit. Aly envoya, 30 minutes après, l'annulation de sa déclaration réglementaire sur EDGAR.

Profits : Des profits de 425 000 USD pour Aly. Une augmentation de la valorisation de la compagnie de 750 millions d'USD.

Moyens : Fausse déclaration dans un site réglementaire boursier officiel.

[214] oir bibliographie [215].
[215] Voir bibliographie [133].
[216] Voir bibliographie [134].
[217] Voir bibliographie [13].
[218] Une des solutions égoïstes pour limiter les éventuels préjudices liés à la désinformation ambiante sur les marchés est en effet toujours d'être le premier. Finalement peu importe que l'information soit vraie ou fausse, ce qui compte c'est de savoir quel va être l'effet de cette information sur le marché ! Comme le dit le vieil adage : « Mieux vaut avoir tort avec le marché que raison contre ».
[219]Voir bibliographie [135].

Cas: EDGAR FITBIT[220]

Résumé : Le 10 novembre 2016, Robert W. Murray a acheté des options d'achat sur le titre FITBIT quelques instants avant de déclarer sur le site EDGAR une fausse offre d'achat (« *Schedule TO-C* ») sur cette société avec un premium de près de 50 % par rapport au prix du marché. Le cours de l'action monta de 10 %, en 10 minutes, et Murray en a profité pour vendre ses options avec profit, seulement 15 minutes après sa fausse déclaration.

Profits : 3100 USD pour le criminel mais une hausse de la valorisation de la société de 913 millions d'USD.

Moyens : Murray a créé un faux compte *email* en usurpant le nom d'un dirigeant pris au hasard sur Internet pour s'enregistrer sur EDGAR. Il a ensuite déclaré ce dirigeant comme directeur financier d'une fausse compagnie (*ABM Capital*) responsable de l'offre d'achat, en falsifiant la signature d'un notaire. Après avoir effectué plusieurs recherches sur les précédents cas poursuivis par la SEC et réalisé l'importance des adresses IP dans l'enquête, Murray a tenté de dissimuler sa véritable identité en utilisant un *proxy* pour son adresse IP. Malheureusement pour lui ; Murray a acheté ses options à partir d'une adresse IP enregistrée au nom de son employeur.

Cas : **EDGAR AVON**[221]

Résumé : Le 14 mai 2015, un trader bulgare dénommé Nedko Nedev a déclaré une fausse offre de rachat du groupe AVON par une fausse entité dénommée *PTG Capital Partners LTD* avec une prime de 181 % (par rapport au cours de clôture de la veille) dans le système réglementaire EDGAR après avoir pris position sur le titre AVON à l'aide de CFD[222]. Une fois la fausse information diffusée, le cours du titre s'est envolé de 20 %, en l'espace de 20 minutes, de 6,6 USD à 8 USD. Le volume d'échange explosa également de 448%. Le 13 décembre 2012 le même mode opératoire avait été utilisé sur le titre *Rocky Mountain* avec un impact de 4,6 % sur le cours de l'action et 1780 % sur le volume et aussi, le 13 mai 2015, sur le titre *Tower Group* avec un impact de 32 % sur le cours de l'action et 1963 % sur le volume d'échange.

Profits : Seulement 5 000 USD de profit personnel mais une hausse de la valorisation d'AVON de près de 600 millions d'USD.

5.2. Prospectives

5.2.1. Le périmètre est très vaste

Si les cas présentés ci-dessus se limitent à la diffusion de fausses informatiosn relative à un émetteur en particulier (sauf pour le cas du Tweet AP avec un effet systémique) et à son impact sur le cours de son action, sans doute parce que le marché boursier des actions reste le marché le plus grand public, il faut garder à l'esprit que le monde boursier est beaucoup plus large et que les possibilités sont extrêmement nombreuses. Pour chaque classe d'actifs (actions, crédit, taux d'intérêts, taux de change, matières premières, énergie, immobilier…), il existe en effet une multitude d'instruments financiers dont le prix peut varier en fonction de plusieurs données.

[220] Voir bibliographie [136].
[221] Voir bibliographie [137].
[222] Le CFD (« Contract for Difference ») est un produit dérivé qui permet une exposition identique aux variations de l'action multipliée par un effet de levier fixé à l'avance.

Prenons par exemple les facteurs influençant le prix[223] d'une sous famille des matières premières plutôt confidentielle comme le bétail[224], parmi eux : les maladies affectant les cheptels, les conditions météorologiques extrêmes des pays producteurs, les habitudes de consommation et le pouvoir d'achat des pays consommateurs, etc… Il semble facile d'imaginer une fausse information pour chacun de ces facteurs et à condition de trouver le moyen de dissémination *ad hoc* (chaque marché ayant ses habitudes et ses sources particulières d'informations) ainsi manipuler le prix des futurs relatifs au bétail.

La classe d'actifs « crédit », en ce qui concerne les sociétés et les émetteurs souverains, est fortement influencée par les *ratings* émis par les agences de notation. Par exemple, le 10 novembre 2011[225], Standard& Poor's, par l'intermédiaire d'un *mail* envoyé à certains de ses abonnés, indiquait par erreur que la note de la dette souveraine française avait été abaissée. L'annonce, qui intervenait alors que la note AAA de la France était clairement menacée, avait fortement secoué les marchés en pleine crise de la dette de la zone euro. L'agence s'était dédouanée ensuite en plaidant que l'erreur avait été provoquée par une confusion de son système informatique… À partir de ce cas et des autres cas d'erreurs très instructifs des agences de notation[226], il est aisé d'imaginer comment ces acteurs pourraient être également la cible de cybermanquement d'initié en subtilisant les notations ou de cyberdiffusion de fausses informations en usurpant l'identité de ces agences ou en modifiant directement les données servant au calcul des notations ou ces dernières elles-mêmes dans leurs systèmes.

Les possibilités sont donc nombreuses et mériteraient une cartographie détaillée.

5.2.2. Les fausses données

Les cas précédents présentaient des fausses informations fabriquées de toute pièce comme des faux communiqués financiers, plus proches de la création d'une fausse histoire classique (« *fake news* ») que de la fausse donnée (« *fake data* »). Mais, dans un monde dont la dépendance aux données croit jour après jour, et ceci est d'autant plus valable pour le monde boursier, comment ne pas imaginer que ces données financières, comme les indices et indicateurs économiques sensibles pour les cybermanquements d'initié définis *supra*, ne soient pas subtilisées, mais plutôt modifiés ou corrompues ?

Une récente étude[227] d'*Accenture* montre à quel point l'intégrité des données est un facteur de risque critique pour les institutions financières. Ainsi, d'après un sondage réalisé auprès de 800 sociétés, plus de la moitié n'aurait pas de système en place robuste pour valider et assurer la qualité de leurs données, alors que la plupart d'entre elles reconnaissent qu'un usage de plus en plus soutenu est fait de ces données pour automatiser les décisions d'investissement, entrainant un risque de manipulation élevé.

Si, comme vu précédemment, il est possible de parfois tromper la vigilance des journalistes employés par les diffuseurs majeurs d'informations financières comme Bloomberg ou Reuters pour qu'ils disséminent inconsciemment de fausses informations, on peut se demander s'il est possible de s'introduire également dans le réseau informatique de ces entreprises pour modifier plus en aval les données de marché diffusées à toute la communauté financière sur les terminaux Bloomberg ou les applications Reuters professionnelles. Vu la présence sur les marchés financiers de ces acteurs (plus de 50 % de part de marché

[223] Voir bibliographie [138].
[224] Des futurs relatifs au bétail sont échangés notamment au Chicago Mercantile Exchange (CME).
[225] Voir bibliographie [139].
[226] Voir bibliographie [140].
[227] Voir bibliographie [141].

à eux deux) et la crédibilité qu'ils apportent aux informations qu'ils diffusent, la cybersécurité de ces deux entreprises et des modes d'acheminement de leurs données aux clients reste une question essentielle, qui, pour l'instant, ne semble pas avoir reçu l'attention qu'elle mérite.

5.2.3. Deep fake et intelligence artificielle

L'imminence de l'intelligence artificielle ou, à tout le moins, de techniques sophistiquées d'apprentissage ou de machine learning, ouvre également de nouvelles perspectives pour la cyberdiffusion de fausse information. La possibilité offerte, et comme toujours facilement accessible grâce aux nombreux tutoriels disponibles sur l'Internet public[228], de pouvoir falsifier des vidéos en « faisant dire n'importe quoi à n'importe qui n'importe comment» (« deepfake ») rend en effet la fausse information encore plus crédible et donc la diffusion de celle-ci encore plus efficace[229]. D'ores et déjà, les gouvernements, notamment américains, s'inquiètent sérieusement du potentiel de désinformation de cette nouvelle menace dans le cadre des élections[230].

Même si aujourd'hui, les vidéos ne semblent pas encore parfaites[231], combien de temps avant qu'une rumeur sur les médias sociaux ne circule avec une vidéo soi-disant cachée du gouverneur de la FED ou de la BCE discutant en privé d'une hausse des taux directeurs ou d'une vidéo montrant un célèbre fonds activiste dévoilant sa prochaine cible ?

Enfin l'apparition de robots « intelligents », propres à simuler sous certaines conditions le comportement humain de manière réaliste, rendra la détection des « social bots » et donc la diffusion de fausse information sans doute encore plus ardue. De même, la présence toujours plus nombreuse de robots conseillers dans les relations entre particuliers et prestataires financiers pose également la question de la cybersécurité de ces derniers, qui, une fois compromis, pourraient être le vecteur de diffusion de fausse information ou de fausses recommandations d'investissements sur des instruments financiers.

[228] Voir bibliographie [142], [143], [144] et [145].
[229] Voir bibliographie [146] et [147].
[230] Voir bibliographie [212] et [213].
[231] voir bibliographie [148].

6. Les cyberattaques sur les bourses

Lorsqu'on parle de cybercriminalité boursière, on pense instinctivement à des cyberattaques sur les places boursières elles-mêmes. Même si les services d'enquête de l'AMF ne seraient pas nécessairement compétents[232], il paraissait difficile d'exclure le sujet, la bourse étant, par essence, le cœur du système.

Dans un sondage réalisé en 2013,[233] auprès de 46 bourses, l'*IOSCO* (« *International Securities Commission Association* ») rapportait d'ailleurs que plus de la moitié avait déjà subi une cyberattaque dans l'année. Les cyberattaques les plus courantes étaient celles qui utilisaient des *malwares* et des dénis de service (DoS) ou des dénis de service distribués (DDoS). Enfin, les cyberattaques subies étaient jugées sans effets sur le bon fonctionnement du marché et n'entraînant qu'un faible coût (inférieur à un million d'USD) pour la bourse. Ainsi, en 2012, une vague d'attaques DDoS menée par des activistes[234], a touché les bourses américaines NYSE, NASDAQ et BATS mais les systèmes de *trading* ont été épargnés[235]. S'il n'existe pas de cas d'attaque DDoS récemment dévoilé contre une bourse[236], les attaques DDoS contre le secteur financier restent toujours efficaces, malgré les dépenses importantes consenties par ce dernier. Ainsi, le 27 et 28 janvier 2018[237], des attaques DDoS, menées par un seul adolescent, avaient ralenti, voire bloqué, les services bancaires en ligne et mobiles d'*ABN Amro*, tout comme ceux de ses consœurs *ING* et *Rabobank*. Plusieurs cas anciens sont néanmoins intéressants à signaler.

Cas : **Bourse de HK 2011**[238]
Cible : Bourse
Résumé : En 2011, une attaque, *a priori* d'origine chinoise, a causé la suspension de cotation de 7 sociétés et même l'arrêt de la bourse de Hong-Kong. L'attaque aurait en effet compromis le site de diffusion de l'information réglementaire officielle de cette bourse empêchant ces 7 sociétés de déclarer leurs résultats par la voie habituelle et les forçant à trouver des moyens valides de diffusion alternative.

Cas : **Bourse de Varsovie 2014**[239]
Cible : Bourse
Résumé : En novembre 2014, la bourse de Varsovie aurait été compromise par une cyberattaque revendiquée par des djihadistes d'ISIS, qui ont pu subtiliser de nombreuses informations confidentielles comme des *mails* ou des plans du réseau informatique interne. Suite à cette attaque, les cybercriminels ont ainsi dévoilé 41 *logins* et mots de passe de courtiers permettant d'accéder au système de *trading*. Apparemment l'attaque n'aurait pas eu d'impact sur le bon fonctionnement du marché, mais elle illustre l'usurpation possible des comptes de *trading* de la bourse.

Cas: «**NASDAQ is owned», Nasdaq 2012**[240]

[232] Suivant la nature et l'effet de l'attaque subie, elle peut être en effet ou non qualifiée de « manipulation de marché ». De plus, en tant qu'opérateur à même d'avoir un impact systémique sur le secteur financier, la bourse a souvent l'attention de plusieurs régulateurs, dont probablement l'ANSSI, l'ACPR et l'AMF.
[233] Voir bibliographie [149].
[234] Voir bibliographie [150].
[235] Si les systèmes de *trading* (« *core engine* » ou « *matching engine* ») sont compromis par les cybercriminels, on imagine aisément ces derniers tirer profit de cette compromission en augmentant ou diminuant « artificiellement » le prix respectivement de leur vente ou de leur achat.
[236] Si ce n'est la toute récente cyberattaque contre la bourse de HongKong survenue le 6 septembre 2019. Voir bibliographie [221]
[237] Voir bibliographie [151].
[238] Voir bibliographie [150] et [152].
[239] Voir bibliographie [153].
[240] Voir bibliographie [154], [155], [156].

Cible : Bourse

Résumé : De mai 2007 à 2011, des hackers russes ont réussi à compromettre le réseau interne informatique du NASDAQ. Les cybercriminels ont d'abord utilisé des injections SQL sur le site du NASDAQ pour obtenir un accès puis installé un *malware* pour obtenir un accès persistant (*backdoor*). Ils n'ont pas subtilisé d'informations particulières si ce n'est des *logins* et mots de passe administrateurs. L'un des hackers aurait écrit à un de ses complices : « *Nasdaq is owned* ». Il semblerait que les systèmes de trading n'aient pas été affectés par l'attaque, laquelle s'est concentrée sur la partie réseau « *corporate* ».

7. Cartographie de la cybercriminalité boursière et des facteurs aggravants et atténuants

8. Conclusion

Depuis plusieurs années, et la presse s'en est souvent fait l'écho, la cybercriminalité a envahi notre monde et représente dorénavant une des menaces majeures. L'analyse approfondie d'une méthodologie d'estimation de son coût, dite de marché et basée sur l'impact moyen d'une cyberattaque sur le cours boursier de la société victime, que différentes études estiment variant entre -1 % et -5 %, montre que les incertitudes autour de la quantification sont extrêmement fortes. Néanmoins, un ordre de grandeur de 0,5 % du PIB mondial peut sembler raisonnable. Quoiqu'il en soit, la cybercriminalité est déjà (ou en passe de le devenir) la forme de criminalité la plus coûteuse et représente presque 10 % de la contribution économique globale d'Internet. Le secteur financier et plus particulièrement la sphère boursière n'échappent pas à cette cybercriminalité, mais il semble plus difficile de leur associer un coût spécifique, en l'absence d'une nouvelle étude plus approfondie.

En excluant explicitement toute cybercriminalité liée aux cryptomonnaies, qui pourrait également être l'objet d'une étude spécifique, la cybercriminalité boursière s'articule autour des trois manquements suivants : cybermanquement d'initié (ex : piratage informatique afin d'obtenir des informations privilégiées), cyberdiffusion de fausses informations financières (ex : création de « faux » sites internet ou fausses rumeurs par les réseaux sociaux influant sur le cours de bourse d'une société cotée) et cybermanipulation de cours (ex : piratage de comptes de *trading* pour mise en place de schéma de type « *pump&dump* »).

L'analyse des cas réels de cybermanquement d'initié a montré que toute la chaîne des acteurs du monde financier (émetteur, banque, avocat, diffuseur d'information, régulateur boursier, bourse…) pouvait être touchée, notamment avec des attaques souvent fondées sur une campagne d'hameçonnage ciblée, avec des documents joints infectés ou des accès non autorisés d'employés IT. Certaines de ces campagnes semblent avoir été orchestrées par des groupes organisés et spécialisés. La monétisation de l'information privilégiée ou des moyens d'accéder à celle-ci sur le *Dark web* reste une question à résoudre, mais il est certain que les fuites de données massives de ces dernières années auront leur rôle à jouer dans les prochains cybermanquements d'initié. Enfin, la multiplication des points d'entrée avec le développement de la mobilité numérique, du *cloud* et de l'IoT ainsi que l'étendue du périmètre des informations privilégiées (par exemple : indicateurs, indices, données économiques sur toutes les classes d'actifs) dont la production et la diffusion n'est pas nécessairement très sécurisée rendront sans doute les cybermanquements d'initiés encore plus attractifs et pourraient faire l'objet d'une cartographie plus détaillée.

Les cas de cybermanipulation de cours relevés découlent principalement de l'intrusion de comptes de trading de particuliers, où le cybercriminel, une fois aux commandes du compte compromis, met généralement en place une stratégie manipulatoire rapide de type « *pump&dump* ». Néanmoins, il existe au moins un cas d'intrusion d'un compte de *trading* professionnel par un groupe organisé et spécialisé dans la cybercriminalité financière. La plupart des applications de trading, mobiles ou fixes, pourrait souffrir de graves lacunes de sécurité. Enfin, les algorithmes étant au cœur des échanges financiers, la compromission de ces derniers ou du chemin de transmission de leurs ordres à la bourse, à des fins manipulatoires parait un des thèmes plausibles à l'avenir.

La cyberdiffusion de fausse information peut, comme les cybermanquements d'initié, toucher plusieurs acteurs de la chaine financière de diffusion, mais les premiers visés sont surtout les diffuseurs d'information financière spécialisée comme Bloomberg ou Reuters, voire parfois les applications des régulateurs boursiers qui recueillent certaines déclarations obligatoires relatives aux sociétés cotées.

Lorsqu'une telle cyberattaque, souvent peu sophistiquée, et dont les motivations sont majoritairement activistes, réussit, les variations de capitalisation boursière engendrées en quelques minutes sont souvent de l'ordre de plusieurs centaines de millions voire plusieurs milliards d'euros, même si les coupe-circuits boursiers les limitent. En revanche, le risque est très faible pour le cybercriminel qui peut facilement conserver son anonymat. C'est pour cela qu'il est fondamental de renforcer les procédures de sensibilisation et de sécurisation des diffuseurs pour éviter tout piratage en amont ou en en aval (directement dans les systèmes). Une étude poussée du niveau de cybersécurité présent chez Bloomberg ou Reuters et des vulnérabilités potentielles serait extrêmement utile. Plusieurs cas ont également utilisé la capacité de dissémination des réseaux sociaux comme Twitter à des fins économiques (campagnes promotionnelles de type « *pump&dump* ») ou activistes. L'automatisation et la rapidité des marchés, dopés aux algorithmes, et ce d'autant plus lorsqu'ils lisent directement les flux de nouvelles, rendent la désinformation encore plus efficace. L'avènement de l'intelligence artificielle avec ses nombreuses possibilités comme les « *deepfake* » ou des « *socialbot*s » intelligents rendra la détection des fausses informations encore plus ardue, et ce d'autant plus que les marchés financiers possèdent de nombreuses classes d'actifs potentiellement inexplorées par les cybercriminels. Enfin, il faut garder à l'esprit que les données et autres indicateurs économiques sensibles peuvent être subtilisés (comme dans les cybermanquement d'initié) mais aussi modifiés à des fins de diffusion de fausse information!

Enfin, les cas de compromission de la bourse elle-même existent et attestent la réalité de la menace, mais ces cas restent anciens et limités à la compromission du réseau interne « corporate », sans impact sur les systèmes de négociation.

Ainsi, cette étude a montré l'étendue de la cybercriminalité boursière, qui touche ou peut toucher toute la chaîne des acteurs du monde financier avec des conséquences extrêmement importantes dans des échelles de temps réduites. L'existence de facteurs aggravants (évolution des technologies, des comportements, spécificités structurelles du monde boursier, facilités du cybercrime) rend cette cybercriminalité boursière encore plus attractive, et ce, dans un contexte où malgré la prise de conscience généralisée du risque cyber et des nouvelles lois relatives à la cybersécurité, à la protection des données personnelles ou aux « *fake news* », la coopération internationale reste difficile et le cadre juridique international encore peu adapté. La sensiblisation et la mobilisation des différents régulateurs internationaux, à l'instar de la SEC qui, dès juillet 2017, créait sa « *cyberunit* » ou de l'AMF, apparaissentt donc primordiale afin d'enrayer cette cybercriminalité boursière.

Ainsi, dans sa cartographie des risques de juillet 2017, l'AMF soulignait l'importance des risques de nature cyber avec un focus spécifique sur le sujet, puis, dans son plan stratégique 2018-2022, elle rappelait l'enjeu important qu'était devenue la cybercriminalité et sa volonté de développer les nouvelles expertises pour y répondre et annonçait en 2019 des contrôles thématiques et courts sur la cybersécurité des sociétés de gestion, cette dernière devenant également intégrée aux contrôles classiques. Enfin, l'AMF participe régulièrement, en règle générale avec la Banque de France et le Trésor, à de nombreux groupes de travail internationaux dédiés à la cybersécurité financière comme le *Cyber Expert Group* du G7, l'*European Systemic Group* de l'ESRB, ou des groupes ad-hoc du *Financial Stability Board (*FSB*)* ou de *l'OICV-IOSCO* (Organisation Internationale des commissions de valeurs) ainsi qu'aux campagnes de remontée d'avis de l'ESMA, l'homologue de l'AMF au niveau européen, sur l'amélioration éventuelle des textes de l'UE liés à la cybersécurité financière. Au niveau européen, on note également la forte implication de la Banque Centrale Européenne (BCE) avec la publication en mai 2018 du cadre de tests de

pénétration TIBER-EU[241] et en décembre 2018 de ses attentes en termes de cyberrésilience pour les infrastructures de marché[242].

L'étude s'étant fondée uniquement sur des données publiques, c'est-à-dire, soit des cas mis en ligne par les autorités judiciaires (principalement américaines), soit par des articles de presse spécialisées sur l'Internet, le panorama n'est certainement pas exhaustif, et ce d'autant plus que beaucoup de cybercrimes restent non détectés ou détectés tardivement[243]. Enfin, le temps des enquêtes étant long, les cas présentés ici sont forcément anciens et ne traduisent donc pas nécessairement l'état actualisé de la cybercriminalité boursière.

Bibliographie et références

1. WORLD ECONOMIC FORUM, *The Global Risks Report 2018 (13th Edition)*. 2018. http://www3.weforum.org/docs/WEF_GRR18_Report.pdf
2. GROUPE DE TRAVAIL INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE, *Protéger les internautes (rapport sur la cybercriminalité)*. Février 2014. http://www.justice.gouv.fr/include_htm/pub/rap_cybercriminalite.pdf
3. BOOS, R. La lutte contre la cybercriminalité au regard de l'action des Etats. Droit. Université de Lorraine, 2016. https://tel.archives-ouvertes.fr/tel-01470150/document
4. GORDON, M.S., *Statement before the House Financial Services Committee*, 14 septembre 2011 https://archives.fbi.gov/archives/news/testimony/cyber-security-threats-to-the-financial-sector
5. NETTITUDE, *Threat Advisory SWIFT Banking*, décembre 2016. https://www.nettitude.com/wp-content/uploads/2016/12/Nettitude-SWIFT-Threat-Advisory-Report-client.pdf
6. MWR INFOSECURITY, *Threat Analysis SWIFT Systems and the SWIFT Customer Security Program* https://www.mwrinfosecurity.com/assets/swift-whitepaper/mwr-swift-payment-systems-v2.pdf
7. AMF, *Cartographie des risques 2017*, 3 juillet 2017 https://www.amf-france.org/Publications/Lettres-et-cahiers/Risques-et-tendances/Archives?docId=workspace%3A%2F%2FSpacesStore%2F50b71ad3-51f9-403e-b884-c92ac8b4b040
8. AMF, *#Supervision2022 : l'AMF présente sa stratégie 2018-2022*, 18 janvier 2018 https://www.amf-france.org/Reglementation/Dossiers-thematiques/l-AMF/Plan-strategique-de-l-AMF/strategies-2018-2022-de-l-autorite-des-marches-financiers
9. https://www.sec.gov/spotlight/cybersecurity-enforcement-actions et https://www.sec.gov/news/press-release/2017-176
10. BERTHIER, T. *Les 3F du HoaxCrash : Fausse donnée, FlashCrash et Forts profits*, Janvier 2017 https://www.chaire-cyber.fr/IMG/pdf/article_hoaxcrash_revise_-_t_berthier_-_chaire_saint-cyr.pdf
11. PELIKS,G. *La cybercriminalité*, Mai 2013 https://www.forumatena.org/files/livresblancs/LaCybercriminalite.pdf
12. LIN, T.C.W. *The New Market Manipulation*, Emory Law Journal.

[241] Voir bibliographie [219].
[242] Voir bibliographie [220].
[243] On pense bien évidemment aux attaques de type APT (menaces persistantes avancées) supposées placer la persistance dans les systèmes comme priorité et donc aussi la capacité à effacer ses traces.

http://law.emory.edu/elj/content/volume-66/issue-6/articles/the-new-market-manipulation.html
13. RENAULT, T. *Market Manipulation and suspicious stock recommendations on Social Media*, 31 Jul 2017 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3010850
14. NASSON,L et SMITH T.N et ZEYTOONIAN, A. *The future of financial crime and enforcement is cyber-based,* K&L Gates*,* 3 janvier 2018 http://www.klgates.com/the-future-of-financial-crime-and-enforcement-is-cyber-based-01-03-2018/
15. MINISTERE DE L'INTERIEUR, *Etat de la menace liée au numérique en 2018*, 20 juin 2018. https://www.interieur.gouv.fr/Le-ministre/Communiques/Etat-de-la-menace-liee-au-numerique-en-2018
16. US GOVERNMENT ACCOUNTABILITY OFFICE, *Costs of crime: experts report challenges estimating costs and suggest improvement to better inform policy decision*, septembre 2017 https://www.gao.gov/assets/690/687353.pdf
17. THE COUNCIL OF ECONOMIC ADVISERS, *The cost of malicious cyber activity to the US Economy*, Février 2018 https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf
18. SCOTT, P. *How much of a problem is cyber-crime in the UK*, 1 novembre 2016 https://www.telegraph.co.uk/news/2016/11/01/how-much-of-a-problem-is-cyber-crime-in-the-uk/
19. https://www.justice.gov/usao-wdwa/victim-witness/victim-info/financial-fraud
20. EDWARDS, *E. DPC receives over 1100 reports of data breaches since start of PIBR rules*, 30 juillet 2018 https://www.irishtimes.com/business/technology/dpc-receives-over-1-100-reports-of-data-breaches-since-start-of-PIBr-rules-1.3580240
21. FIREEYE, *special report M-Trends 2018* https://www.fireeye.com/content/dam/collateral/en/mtrends-2018.pdf
22. PWC, *Managing cyber risks in an interconnected world*, 30 septembre 2014 https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf
23. KOPPE et KAFFENBERGER, L et WILSON Christopher. *Cyber risk, market failures and financial stability*, IMF Working Paper, 7 aout 2017. https://www.imf.org/en/Publications/WP/Issues/2017/08/07/Cyber-Risk-Market-Failures-and-Financial-Stability-45104
24. MCAFEE (CSIS), *Economic impact of cybercrime*, fevrier 2018 https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf
25. https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-comparison-france-en.pdf
26. RIOUX, P. La cybercriminalité coute 3,36 milliards d'euros aux entreprises françaises, 8 mars 2017 https://www.ladepeche.fr/article/2016/03/08/2299605-cybercriminalite-coute-3-36-milliards-euros-entreprises-francaises.html
27. MANYIKA J. et ROXBURGH C. *The great transformer: the impact of Internet on economic growth and prosperity*, McKinsey Global Institute, October 2011 https://www.mckinsey.com/~/media/McKinsey/Industries/High%20Tech/Our%20Insights/The%20great%20transformer/MGI_Impact_of_Internet_on_economic_growth.ashx
28. INTERNET ASSOCIATION, *New Report calculates the size of the Internet Economy*, 10 décembre 2015 https://internetassociation.org/121015econreport/
29. GLOBAL FINANCIAL INTEGRITY, *Transnational crime and the developing world*, Mars 2017 http://www.gfintegrity.org/wp-content/uploads/2017/03/Transnational_Crime-final.pdf
30. NATIONAL CRIME AGENCY, *Cyber crime assessment 2016*, 7 juillet 2016 http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file
31. JUNIPER RESEARCH, *Cybercrime to cost global business over $8 trillion in the next 5 years*, 30 mai 2017 https://www.juniperresearch.com/press/press-releases/cybercrime-to-cost-global-business-over-$8-trn

32. CYBERSECURITY VENTURES, *Cybercrime Damages $6 Trillion by 2021,* 16 Octobre 2017
https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/
33. CGI, *The cyber-value connection*
https://www.cgi.com/sites/default/files/2018-08/cybervalueconnection_full_report_final_lr.pdf
34. KAMIYA, S et all. *What is the Impact of Successful Cyberattacks on Target Firms* ?, 7 mars 2018
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3135514
35. CENTRIFY et PONEMON, *The impact of data breaches on reputation & share value*, Mai 2017
https://www.centrify.com/media/4772757/ponemon_data_breach_impact_study_uk.pdf
36. AMIR E. et LEVI S. et LIVNE,T., *Do firms underreport information on cyber-attacks ? Evidence from capital markets*, Mai 2017
https://sites.insead.edu/facultyresearch/research/file.cfm?fid=60951
37. NUSCA, A. *Equifax Stock has plunged 18,4% since it revealed massive breach*, 11 septembre 2017.
http://fortune.com/2017/09/11/equifax-stock-cybersecurity-breach/
38. MARCOGLIESE,P et MUKHI R., *Untangling the Tangled Web of cybersecurity disclosure requirements: a practical guide*, 17 juin 2018
https://corpgov.law.harvard.edu/2018/06/17/untangling-the-tangled-web-of-cybersecurity-disclosure-requirements-a-practical-guide/
39. SOLOMON C et all, *Failure to Disclose a cybersecurity breach*, 17 mai 2018.
https://corpgov.law.harvard.edu/2018/05/17/failure-to-disclose-a-cybersecurity-breach/#more-106859
40. PONEMON Institute et ACCENTURE, *2017 Cost of cybercrime study*
https://www.accenture.com/t20170926T072837Z__w__/us-en/_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf
41. BARETT, B. *The wild inner workings of a billion-dollar hacking group*, 8 janvier 2018.
https://www.wired.com/story/fin7-wild-inner-workings-billion-dollar-hacking-group/
42. DEPARTEMENT OF JUSTICE, *Three members of notorious international cybercrime group "fin7" in custody for role in attacking over 100 US companies*, 1 aout 2018
https://www.justice.gov/opa/pr/three-members-notorious-international-cybercrime-group-fin7-custody-role-attacking-over-100
43. FIREEYE, *On the hunt for FIN7: Pursuing an enigmatic and evasive global criminal operation*, 1 aout 2018.
https://www.fireeye.com/blog/threat-research/2018/08/fin7-pursuing-an-enigmatic-and-evasive-global-criminal-operation.html
44. LE MONDE, *Les Etats-Unis accusent trois ukrainiens d'avoir piraté 15 millions de cartes de crédit*, 2 aout 2018
https://www.lemonde.fr/pixels/article/2018/08/02/les-etats-unis-accusent-trois-ukrainiens-d-avoir-pirate-15-millions-de-cartes-de-credit_5338611_4408996.html
45. https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/
46. FIREEYE, *Unsealing the deal : cyber threats to mergers and acquisitions persist in a hot market,* 23 aout 2016
https://www.fireeye.com/blog/threat-research/2016/08/unsealing_the_deal.html
47. FIREEYE, *Hacking the street? FIN4 likely playing the market,* 2014.
https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-fin4.pdf
48. LYNCH, S et MENN J., *Exclusive : SEC hunts hackers who stole corporate emails to trade stocks*, 23 juin 2015
https://www.reuters.com/article/us-hackers-insidertrading/exclusive-sec-hunts-hackers-who-stole-corporate-emails-to-trade-stocks-idUSKBN0P31M720150623?feedType=RSS&feedName=topNews
49. SEC vs JONATHAN LY
https://www.sec.gov/litigation/complaints/2016/comp-pr2016-256.pdf
50. SEC vs LOHUS HAAVEL & VIISEMANN, OLIVER PEEK, and KRISTJAN LEPIK
https://www.sec.gov/litigation/complaints/comp19450.pdf

51. RAJ CHANDEL'S BLOG, *5 ways to crawl a website*, 16 juillet 2017
http://www.hackingarticles.in/5-ways-crawl-website/
52. DEPARTMENT OF JUSTICE, *hackers sentenced to 30 months in prison for role in largest known computer hacking and securities fraud scheme*, 22 mai 2017
https://www.justice.gov/usao-nj/pr/hacker-sentenced-30-months-prison-role-largest-known-computer-hacking-and-securities
53. SEC vs DUBOVOY and all
https://www.sec.gov/litigation/complaints/2015/comp-pr2015-163.pdf
54. SEC, *SEC charges nine additional defendants in hacked news release*, 18 février 2016
https://www.sec.gov/litigation/litreleases/2016/lr23471.htm
55. SEC, *traders agrees to settle claims relating to hacked news release scheme; SEC's recovery to date in connection with the scheme exceeds $52 million*, 4 mai 2016
https://www.sec.gov/litigation/litreleases/2016/lr23530.htm
56. ASIC, *18-136MR IT consultant charged with gaining unauthorized access to dat and insider trading*, 14 mai 2018.
https://asic.gov.au/about-asic/media-centre/find-a-media-release/2018-releases/18-136mr-it-consultant-charged-with-gaining-unauthorised-access-to-data-and-insider-trading/
57. DEPARTMENT OF JUSTICE, *Five individual charged with participating in three insider trading schemes generating more than $5 million I profits on inside information misappropriated from an investment bank*, 16 aout 2017
https://www.justice.gov/usao-sdny/pr/five-individuals-charged-participating-three-insider-trading-schemes-generating-more-5
58. SEC vs IAT HONG, BO ZHENG, and HUNG CHIN
https://www.sec.gov/litigation/complaints/2016/comp-pr2016-280.pdf
59. SEC, *SEC chairman clayton issues statement on cybersecurity*, 20 septembre 2017
https://www.sec.gov/news/press-release/2017-170
60. SEC, *Testimony on Oversight of the US SEC,* 21 juin 2018
https://www.sec.gov/news/testimony/testimony-oversight-us-securities-and-exchange-commission#_ftn1
61. ROBERTS, JJ. *Fake SEC emails targets execs for inside information*, 7 mars 2017
http://fortune.com/2017/03/07/sec-phishing/
62. FIREEYE, *FIN7 spear phishing campaign targets personnel involved in SEC filings*, 7 mars 2017
https://www.fireeye.com/blog/threat-research/2017/03/fin7_spear_phishing.html
63. TALOS, *Spoofed SEC emails distribute evolved DNSMssenger*, 11 octobre 2017
http://blog.talosintelligence.com/2017/10/dnsmessenger-sec-campaign.html
64. https://wraithhacker.com/2017/10/11/more-info-on-evolved-dnsmessenger/
65. SPRING, T. *New Fileless attack using dns queries to carry out powershell commands*, 4 mars 2017
https://threatpost.com/new-fileless-attack-using-dns-queries-to-carry-out-powershell-commands/124078/
66. REUTERS, *Exclusive: NASDAQ hackers spied on company boards*, 20 octobre 2011
https://www.reuters.com/article/us-nasdaq-hacking-idUSTRE79J84T20111020
67. ARSTECHNICA, *How elite hackers (almost) stole the NASDAQ*, 17 juillet 2014
https://arstechnica.com/information-technology/2014/07/how-elite-hackers-almost-stole-the-nasdaq/
68. REDOWL, *Monetizing the Insider*
http://itzashita.ru/wp-content/uploads/2017/05/RedOwl_Intsights_Report.pdf
69. SIFMA CYBERSECURITY, *Insider threat best practices guide*, 2nd edition, Février 2018
https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf
70. REPKNIGHT, *Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms*, janvier 2018
https://www.repknight.com/wp-content/uploads/2018/01/White-Paper-Securing-the-Law-Firm-January-2018-Website-LM.pdf

71. SECURITYWEEK, *Hackers will break into email, social media accounts for just $129*, 6 avril 2016
https://www.securityweek.com/hackers-will-break-email-social-media-accounts-just-129
72. UNDERNEWS, *Telegram, le nouveau médium de choix de la cybercriminalité*, 9 mai 2018
https://www.undernews.fr/hacking-hacktivisme/telegram-le-nouveau-medium-de-choix-de-la-cybercriminalite.html?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+undernews%2FoCmA+%28UnderNews%29
73. CPR*, Telegram: cyber crime's channel of choice,*
https://research.checkpoint.com/telegram-cyber-crimes-channel-choice/
74. SEC vs JUN YING
https://www.sec.gov/litigation/complaints/2018/comp-pr2018-40.pdf
75. MARKETWATCH, *Short seller muddy waters renews claims of St. Jude Medical cyber vulnerabilities*, 19 octobre 2016.
https://www.marketwatch.com/story/short-seller-muddy-waters-renews-claims-of-st-jude-medical-cyber-vulnerabilities-2016-10-19
76. THE WASHINGTON POST, The cybersecurity 202: a wake up call. OPM data stolen years ago surfacing now in financial fraud case, 20 juin 2018
https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2018/06/20/the-cybersecurity-202-a-wake-up-call-opm-data-stolen-years-ago-surfacing-now-in-financial-fraud-case/5b2924ca1b326b3967989b66/?noredirect=on&utm_term=.e1356c6af0a1
77. https://data.sca.isr.umich.edu/survey-info.php.
78. CNBC, *Thomson reuters gives elite traders early advantage*, 12 juin 2013
https://www.cnbc.com/id/100809395
79. GARTNER, *Gartner says 8,4 Billion connected things will be in use in 2017*, up 31 percent from 2016, 7 février 2017
https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016
80. HAGER, S. *Les voyageurs d'affaire, portes d'entrée des hackers* . Option Finance n°1467. 18 juin 2018
81. TECHRADARPRO, *why you should avoid hotel Wi-Fi like the plague*, 7 mars 2018
https://www.techradar.com/news/networking/wi-fi/why-you-should-avoid-hotel-wi-fi-like-the-plague-1292555/2
82. SECURITY RESEARCH LABS, *USB peripherals can turn against their users*
https://srlabs.De/bites/usb-peripherals-turn/
83. KHANDELWAL S., *Hackers can silently control Siri, Alexa & Other voice assistants using ultrasound*, 6 septembre 2017
http://thehackernews.com/2017/09/ai-digital-voice-assistants.html
84. SEC vs JOSEPH P. WILLNER
https://www.sec.gov/litigation/complaints/2017/comp-pr2017-202.pdf
85. SEC vs IDRIS D.MUSTAPHA
https://www.sec.gov/litigation/complaints/2016/comp-pr2016-127.pdf
86. SEC vs IGORS NAGAICEVS
https://www.sec.gov/litigation/complaints/2012/comp22238.pdf
87. SEC vs BROCO INVESTMENTS, INC and VALERY MALTSEV
https://www.sec.gov/litigation/complaints/2010/comp21452.pdf
88. LIPOVSKY R., *Corkow: analysis of a business-oriented banking Trojan*, 27 février 2014.
https://www.welivesecurity.com/2014/02/27/corkow-analysis-of-a-business-oriented-banking-trojan/
89. GROUP-IB REPORT: *Analysis of attacks against trading and bank card systems*
https://www.group-ib.ru/brochures/Group-IB-Corkow-Report-EN.pdf
90. BOUTIN, JI et CHEREPANOV, A. *Modern attacks against Russian financial institutions*, Virus bulletin conference October 2016
https://www.virusbulletin.com/uploads/pdf/magazine/2016/VB2016-Boutin-Cherepanov.pdf

91. POISTIVE TECHNOLOGIES, *Cobalt strikes back: an evolving multinational threat to finance*, 1 aout 2017 http://blog.ptsecurity.com/2017/08/cobalt-group-2017-cobalt-strikes-back.html
92. ROMANIA INSIDER, *Romanian financial institutions targeted by big cyber-attacks*, 20 aout 2018 https://www.romania-insider.com/financial-institutions-cyber-attacks/
93. DEPARTMENT OF JUSTICE, *Attorney General and Manhattan US Attorney announce charges stemming from massive network intrusions at US Financial Institutions, US Brokerage firms, Major News Publication and other companies*, 10 novembre 2015 https://www.justice.gov/opa/pr/attorney-general-and-manhattan-us-attorney-announce-charges-stemming-massive-network
94. REUTERS, *UPDATE 4-US charges three in huge cyberfraud targeting JPMorgan*, others, 10 novembre 2015 https://www.reuters.com/article/hacking-indictment-idUSL1N13518P20151110
95. SEC vs JOSHUA SAMUEL AARON, GERY SHALON, and ZVI ORENSTEIN. https://www.sec.gov/litigation/complaints/2015/comp-pr2015-152.pdf
96. REUTERS, HongKong police struggle to stop hacking spree, 15 février 2017 https://in.reuters.com/article/cyber-brokerages-hongkong/hong-kong-police-struggle-to-stop-brokerage-hacking-spree-idINKBN15U0BA
97. HONGKONG CASE LAW*, fast track holdings ltd vs BOCI securities ltd and others*, 12 novembre 2016 https://www.hongkongcaselaw.com/fast-track-holdings-ltd-v-boci-securities-ltd-and-others/
98. SFC, *SFC notifies the industry of cybersecurity review on internet/mobile trading systems*, 13 octobre 2013 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=16EC46
99. SFC, *Consultation paper on proposals to reduce and mitigate hacking risks associated with Internet trading*, Mai 2017 https://www.sfc.hk/edistributionWeb/gateway/EN/consultation/openFile?refNo=17CP4
100. SOUTH CHINA MORNING POST, *SFC orders tighter safeguards to stop hackers invading online trading accounts*, 27 octobre 2017 https://www.scmp.com/business/article/2117363/sfc-orders-tighter-safeguards-stop-hackers-invading-online-trading-accounts
101. SFC, *Circular to intermediaries receiving client orders through instant messaging*, 4 mai 2018 https://www.sfc.hk/edistributionWeb/gateway/EN/circular/doc?refNo=18EC30
102. ESET, *State of cybersecurity in APAC: small businesses, big threats* https://www.welivesecurity.com/wp-content/uploads/2017/10/State-of-cybersecurity-in-APAC_Small-Businesses-Big-Threats.pdf
103. KREBSON SECURITY, *Target hackers broke in via HVAC Company*, 14 février 2014 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company
104. HERNANDEZ, A. *Are you trading stocks securely? Exposing security flaws in trading technologies*. IOActive, juillet 2018 https://ioactive.com/wp-content/uploads/2018/08/Are-You-Trading-Stocks-Securely-Exposing-Security-Flaws-in-Trading-Technologies.pdf
105. https://www.ft.com/content/d81f96ea-d43c-11e7-a303-9060cb1e5f44
106. KOPPENHEFFER, *M. Everything you need to know about the Knight Capital Meltdown*, 14 septembre 2012. https://www.fool.com/investing/general/2012/09/14/everything-you-need-to-know-about-the-knight-capit.aspx
107. THE TECHNOLOGY EVANGELIST, *Security: DARPA, HFT & FINANCIAL MARKETS*, 18 décembre 2017 https://technologyevangelist.co/2017/12/18/security-darpa-hft-financial-markets
108. SNYDER, *B. Hackers find new way to cheat on Wall Street—to everyone's peril*, INFOWORLD, 6 janvier 2011 https://www.infoworld.com/article/2624981/network-monitoring/hackers-find-new-way-to-cheat-on-wall-street----to-everyone-s-peril.html
109. THE HISTORY OF PRESS*, Napoleon is dead! The great stock exchange fraud of 1814* https://www.thehistorypress.co.uk/articles/napoleon-is-dead-the-great-stock-exchange-fraud-of-1814/

110. LE MONDE, *les grandes entreprises de la Silicon Valley se rencontrent pour parler de la désinformation*, 24 aout 2018 https://www.lemonde.fr/pixels/article/2018/08/24/les-grandes-entreprises-de-la-silicon-valley-se-rencontrent-pour-parler-de-la-desinformation_5345665_4408996.html
111. MINISTERE DE LA CULTURE, *les enjeux de la loi contre la manipulation de l'information*, 4 juillet 2018. http://www.culture.gouv.fr/Actualites/Les-enjeux-de-la-loi-contre-la-manipulation-de-l-information
112. FUTURISM*, Ethereum lost $4 Billion in market value due to fake "fatal car crash"*, 27 juin 2017 https://futurism.com/ethereum-lost-4-billion-in-market-value-due-to-fake-fatal-car-crash/
113. SEC vs MARK S. JAKOB https://www.sec.gov/litigation/litreleases/lr16671.htm
114. DUFFY, *A. Fake press release wipes $314 million of Whitehaven*, Australian Mining, 7 janvier 2013 https://www.australianmining.com.au/news/fake-press-release-wipes-314-million-off-whitehaven/
115. MARTIN, B et SPENCE, P. *G4S shares knocked by elaborate hoax regarding company's finances*, 12 novembre 2014. http://www.telegraph.co.uk/finance/markets/11226463/G4S-shares-knocked-by-elaborate-hoax-regarding-companys-finances.html
116. ANONYME, *Prank the pranksters! Playing around with information and fakes in the age of immaterial capitalism* https://foolcapitalism.espivblogs.net/files/2015/10/PrankThePrankster.pdf
117. THOMPSON M et KOTTASOVA, I, *How a big Italian bank was slammed by an hoax*, 24 avril 2015 https://money.cnn.com/2015/04/24/investing/italian-bank-hoax/
118. https://www.linkiesta.it/it/article/2015/04/24/il-finto-comunicato-che-ha-fatto-tremare-il-titolo-di-intesa-sanpaolo/25628/
119. http://www.ilgiornale.it/news/politica/email-far-crollare-mercato-i-no-tav-attaccano-banca-italiana-1120580.html
120. THE GUARDIAN, *Twitter's shares jump after fake story company's $31bn takeover offer*, 14 juillet 2015 https://www.theguardian.com/technology/2015/jul/14/twitter-shares-fake-story-bloomberg
121. FILIPPONE D., *Vinci dégringole en bourse suite à un hoax*, 23 novembre 2016 https://www.lemondeinformatique.fr/actualites/lire-vinci-degringole-en-bourse-suite-a-un-hoax-66589.html
122. JACQUE, P. *Comment le groupe Vinci victime d'un « hoax » a chuté en Bourse*, 23 novembre 2016 https://www.lemonde.fr/economie-francaise/article/2016/11/23/comment-le-groupe-vinci-victime-d-un-hoax-a-chute-en-bourse_5036269_1656968.html
123. AMF, *l'AMF présente l'avancement de ses travaux à la suite de la diffusion d'une fausse information relative au titre Vinci*, 23 février 2017 https://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2017.html?docId=workspace%3A%2F%2FSpacesStore%2Ffba06651-ed84-4e46-a9db-1876b4330712
124. SELYUKH, *A. Hackers send fake market moving AP tweet on White House explosions*, 23 avril 2013 https://www.reuters.com/article/net-us-usa-whitehouse-ap/hackers-send-fake-market-moving-ap-tweet-on-white-house-explosions-idUSBRE93M12Y20130423
125. https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/?utm_term=.e0629cdeaadf
126. SEC vs JAMES ALAN CRAIG https://www.sec.gov/litigation/complaints/2015/comp-pr2015-254.pdf
127. https://seekingalpha.com/article/2274553-cynk-technology-promoters-push-market-cap-to-655-million-despite-39-in-assets-and-no-revenue-100-percent-downside?page=1
128. http://promotionstocksecrets.com/cynk-aftermath-putting-together-pieces-puzzle/
129. SEC vs PHILIP THOMAS KUEBER https://www.sec.gov/litigation/complaints/2015/comp-pr-2015-157.pdf
130. CNET, *Facebook deleted 583 million fake accounts in the first three months of 2018*, 15 mai 2018 https://www.cnet.com/news/facebook-deleted-583-million-fake-accounts-in-the-first-three-months-of-2018/

131. NEWBERG M. *As many as 48 million Twitter accounts aren't people, says study*. 10 mars 2017
https://www.cnbc.com/2017/03/10/nearly-48-million-twitter-accounts-could-be-bots-says-study.html
132. *The DARPA Twitter Bot Challenge*, 21 avril 2016
https://arxiv.org/abs/1601.05140
133. HUET S., *Sur twitter le faux plus fort que le vrai*, 8 mars 2018.
http://huet.blog.lemonde.fr/2018/03/08/sur-twitter-le-faux-plus-fort-que-le-vrai/
134. SEC, *Updated investor Alert: Social Media and investing—Stock Rumors*, 6 février 2017
https://www.sec.gov/oiea/investor-alerts-bulletins/ia_rumors.html
135. SEC vs NAUMAN A. ALY
https://www.sec.gov/litigation/complaints/2016/comp-pr2016-95.pdf
136. SEC vs ROBERT W.MURRAY
https://www.sec.gov/litigation/complaints/2017/comp23836.pdf
137. SEC vs PTG CAPITAL PARTNERS, NEDKO NEDEV et all
https://www.sec.gov/litigation/complaints/2015/comp-pr2015-110.pdf
138. http://materials-risk.com/livestock-prices-top-10-important-drivers/
139. LEXPRESS, *Standard&Poor's sanctionnée pour avoir dégradé la France par erreur*, 5 juin 2014
https://lexpansion.lexpress.fr/actualite-economique/standard-poor-s-reprimande-pour-avoir-degrade-la-france-par-erreur_1548720.html
140. NICOLAS, *A. Les trois plus grosses bourdes des agences de notation*, 11 novembre 2011
https://www.francetvinfo.fr/economie/bourse/marches/les-trois-plus-grosses-bourdes-des-agences-de-notation_25721.html
141. FINEXTRA, '*Fake data' will make banks vulnerable-Accenture*, 20 avril 2018
https://www.finextra.com/newsarticle/31978/fake-data-will-make-banks-vulnerable---accenture?utm_medium=dailynewsletter&utm_source=2018-4-23&member=42526
142. https://www.youtube.com/watch?v=cQ54GDm1eL0
143. https://goberoi.com/exploring-deepfakes-20c9947c22d9
144. https://www.deepfakes.club/best-hardware-software-deepfakes/
145. https://www.alanzucconi.com/2018/03/14/introduction-to-deepfakes/
146. TUAL, *M. Du porno aux fausses informations, l'intelligence artificielle manipule désormais la vidéo*, 8 février 2018
https://www.lemonde.fr/pixels/article/2018/02/04/du-porno-aux-fausses-informations-l-intelligence-artificielle-manipule-desormais-la-video_5251535_4408996.html
147. COURRIER INTERNATIONAL, Vous n'avez encore rien vu ! Quand la réalité s'effondre, Jeudi 23 Aout 2018
http://lirelactu.fr/source/courrier-international/b64b4654-ada4-4f5a-b0d6-4966dea55a41
148. FINANCIAL TIMES, *if you thought fake news was a problem, wait for deepfakes*
https://www.ft.com/content/8e63b372-8f19-11e8-b639-7680cedcc421
149. OICV-IOSCO, Cyber-crime, securities markets and systemic risk, 16 juillet 2013
https://www.iosco.org/research/pdf/swp/Cyber-Crime-Securities-Markets-and-Systemic-Risk.pdf
150. PROLEXIC, *DDOS Attacks against global markets*, 2014
https://www.akamai.com/de/de/multimedia/documents/content/ddos-attacks-against-global-markets-white-paper.pdf
151. HOFMANS,T. *Teenager suspected of crippling Dutch banks with DDoS attacks*, 8 février 2018
https://www.computerweekly.com/news/252434665/Teenager-suspected-of-crippling-Dutch-banks-with-DDoS-attacks
152. FINANCIAL TIMES, *HongKong echange hit by hackers*
https://www.theglobeandmail.com/report-on-business/international-business/hong-kong-exchange-hit-by-hackers/article599797/
153. BENNET C, *Hackers breach the warsaw stock exchange*, The Hill, 24 octobre 2014
http://thehill.com/policy/cybersecurity/221806-hackers-breach-the-warsaw-stock-exchange

154. USA vs VLADIMIR DRINKMAN, ALEKSANDR KALININ et all
https://www.justice.gov/sites/default/files/opa/press-releases/attachments/2015/02/18/drinkman_vladimir_et_al_indictment_comp.pdf
155. DEPARTMENT OF JUSTICE, *Russian national charged in largest known data breach prosecution extradited to United States*, 17 février 2015
https://www.justice.gov/opa/pr/russian-national-charged-largest-known-data-breach-prosecution-extradited-united-states
156. GOODIN, D. *"NASDAQ is owned" five men charged in largest financial hack ever*, 25 juillet 2013
https://arstechnica.com/information-technology/2013/07/nasdaq-is-owned-five-men-charged-in-largest-financial-hack-ever/
157. WEF,*The new physics of Financial Services*, Aout 2018
http://www3.weforum.org/docs/WEF_New_Physics_of_Financial_Services.pdf
158. ZORZ, Z. *The percentage of open source code in proprietary apps in rising*, 22 mai 2018
https://www.helpnetsecurity.com/2018/05/22/open-source-code-security-risk/
159. ECHENNE, F. Les risques d'une circulation non maîtrisée des flux financiers et informationnels sur Internet, Cahiers de la sécurité et de la Justice n°42, 8 juin 2018
160. Nessim Aît-Kacimi, *Comment les cyberpirates ukrainiens font trembler WallStreet*, Article des Echos, 13 mars 2019
161. https://www.lesechos.fr/2017/10/le-cyber-est-un-meta-risque-qui-touche-tous-les-metiers-de-lentreprise-184557
162. https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline
163. https://www.securityinsider-wavestone.com/2016/06/retour-sur-laffaire-swift-synthese-des.html
164. https://www.afg.asso.fr/wp-content/uploads/2018/12/2018_10_18_Cybersécurité_Enquete-AFG_octobre-2018_site.pdf
165. https://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
166. https://www.bis.org/cpmi/publ/d146.pdf
167. https://www.esma.europa.eu/sites/default/files/library/jc_2019_26_joint_esas_advice_on_ict_legislative_improvements.pdf
168. https://www.swift.com/resource/how-cyber-attackers-could-target-worlds-financial-markets
169. https://www.sec.gov/news/press-release/2018-22
170. https://www.sec.gov/news/press-release/2018-71
171. Rapports financiers annuels :
https://www.saint-gobain.com/sites/sgcom.master/files/fy-2017-fra_a.pdf
http://s1.q4cdn.com/714383399/files/oar/2017/AnnualReport2017/AnnualReport2017flat/docs/FedEx_2017_Annual_Report.pdf
https://www.maersk.com/-/media/ml/about/sustainability/20180209-a-p-moller-maersk-annual-report.pdf
https://ir.mondelezinternational.com/news-releases/news-release-details/mondelez-international-reports-2017-results
http://s21.q4cdn.com/488056881/files/doc_financials/2017/2017-Form-10-K_FINAL-wo-Exhibits_Filed-022718.pdf
172. https://www.statista.com/chart/12707/largest-known-crypto-currency-thefts/
173. KIRK S. Satellites and sensitive sheep blur insider trading ,Financial Times, 29 Novembre 2017.
174. https://www.zdnet.com/article/black-hat-hackers-white-collar-criminals-snuggle-up-to-operate-insider-trading-schemes/
175. https://www.fbi.gov/news/stories/chinese-hackers-indicted-122018
176. https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion
177. https://www.theverge.com/2018/8/22/17716622/sec-business-wire-hack-stolen-press-release-fraud-ukraine
178. https://www.sec.gov/news/press-release/2019-1
179. https://www.sec.gov/litigation/complaints/2019/comp-pr2019-1.pdf

180. https://www.zdnet.com/article/oklahoma-gov-data-leak-exposes-millions-of-department-files-fbi-investigations/
181. https://www.lemondeinformatique.fr/actualités/lire-shodan-moteur-de-recherche-total-de-l-internet-71919.html
182. https://www.amf-france.org/Actualites/Communiques-de-presse/AMF/annee-2018?docId=workspace%3A%2F%2FSpacesStore%2F3d58f35b-f448-438e-9923-cd6e8e903fc0
183. https://www.timesofmalta.com/articles/view/20190225/local/how-bov-hackers-got-away-with-13-million.702800
184. https://asic.gov.au/online-services/service-availability/scams-targeting-asic-customers/
185. https://www.darkreading.com/vulnerabilities---threats/new-report-details-rise-spread-of-email-based-attacks/d/d-id/1333375
186. https://www.bleepingcomputer.com/news/security/over-80-percent-of-all-phishing-attacks-targeted-us-organizations/
187. https://www.gao.gov/assets/700/694158.pdf
188. https://yle.fi/uutiset/osasto/news/cyber-attack_shuts_finnish_ministry_jobs_site/10518762
189. http://www.globalsecuritymag.fr/Les-cyberattaques-visant-les,20190306,85113.html
190. http://www.bromium.com/social-media-platforms-cybercrime-economy/
191. http://globbsecurity.fr/office-365-ligne-de-mire-cybercriminels-44303/
192. https://www.solutions-numeriques.com/cyberattaques-office-365-et-google-g-suite-de-plus-en-plus-vises/
193. https://www.pcworld.com/article/3235484/what-the-kaspersky-antivirus-hack-really-means.html
194. https://www.lemonde.fr/pixels/article/2018/10/04/les-pays-bas-revelent-une-operation-d-espionnage-russe-sur-leur-territoire_5364712_4408996.html
195. https://english.defensie.nl/downloads/publications/2018/10/04/gru-close-access-cyber-operation-against-opcw
196. https://www.lemonde.fr/pixels/article/2018/10/04/espionnage-la-chine-accusee-d-avoir-installe-des-micropuces-dans-des-serveurs-utilises-par-apple-et-amazon_5364769_4408996.html
197. https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies
198. https://www.zdnet.com/article/crims-not-spooks-dominate-cybersecurity-threats-sophos-ceo/
199. https://www.difesaesicurezza.com/en/cyber-en/the-cybercrime-group-carbanak-aka-cobalt-and-fin7-is-not-yet-defeated/
200. https://securelist.com/ksb-cyberthreats-to-financial-institutions-2019-overview-and-predictions/88944/
201. https://www.lesechos.fr/2018/03/cybercriminalite-le-cerveau-du-gang-des-carbanak-arrete-987505
202. https://www.europol.europa.eu/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain
203. https://news.8btc.com/alert-lazarus-hacker-group-continues-targeting-crypto-using-faked-trading-software
204. https://www.smh.com.au/national/nsw/jonathan-moylan-avoids-jail-term-for-fake-anz-media-release-about-whitehaven-coal-20140725-zwwe7.html
205. https://www.smh.com.au/business/dont-believe-the-hype-over-the-cost-of-whitehaven-hoax-20130115-2crh1.html
206. https://www.reuters.com/article/us-fingerprint-samsung/swedish-tech-company-caught-in-hoax-samsung-bid-idUSBRE99A07N20131011
207. https://qz.com/134493/one-fake-press-release-created-200-million-today-and-another-one-made-it-disappear/
208. https://www.reuters.com/article/immunovaccine-regulator-hoax/trades-in-immunovaccine-shares-to-be-undone-after-hoax-spurs-30-pct-jump-idUSL1N0W523G20150303
209. https://www.benzinga.com/news/15/02/5283736/immunovaccine-up-24-on-deal-with-gilead-sciences
210. https://www.fnlondon.com/articles/blackrock-targeted-by-fake-ceo-letter-20190116
211. https://www.lemonde.fr/pixels/article/2019/02/07/whatsapp-supprime-2-millions-de-comptes-par-mois-pour-lutter-contre-les-fausses-informations_5420513_4408996.html
212. https://edition.cnn.com/2019/01/28/tech/deepfake-lawmakers/index.html.
213. https://www.washingtonexaminer.com/news/white-house/the-deep-fake-threat

214. https://www.amf-france.org/Reglementation/Dossiers-thematiques/Fintech/Vers-un-nouveau-regime-pour-les-crypto-actifs-en-France
215. https://www.vox.com/2018/1/23/16923276/facebook-twitter-russia-interference-congress-release-the-memo
216. https://siecledigital.fr/2019/07/23/scandale-equifax-la-societe-recoit-une-amende-de-700-millions-de-dollars
217. https://www.journaldugeek.com/2019/07/25/facebook-amende-record-sans-consequence/
218. https://www.fsb.org/2018/11/cyber-lexicon/
219. https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
220. https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf
221. https://www.finextra.com/newsarticle/34352/hong-kong-exchange-suffers-cyber-attack

INDEX