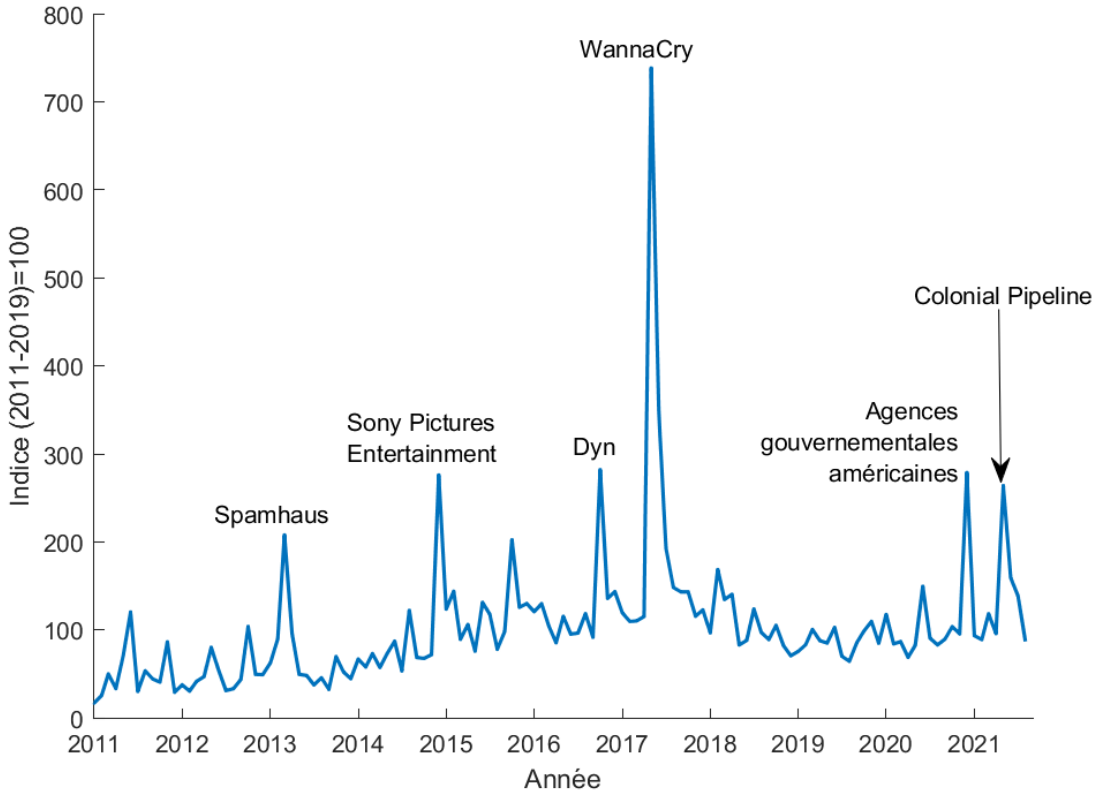
Une mesure de l'évolution du risque cyber

Par Stéphane Lhuissier et Fabien Tripier

Après la crise financière de 2008, la crise sanitaire de 2020, la prochaine crise économique mondiale sera-t-elle cyber ? Le risque cyber constitue une réelle menace pour l'économie face à laquelle les autorités sont mobilisées. Ce billet présente un indicateur permettant de suivre quotidiennement l'évolution de ce risque à partir des échanges sur le réseau social Twitter.

Graphique 1 – Évolution du risque cyber au cours de la dernière décennie



Source : Twitter et calcul des auteurs.

Avec la digitalisation et la transformation du système économique et financier, le risque d'une crise majeure émanant du cyberespace est à prendre au sérieux. C'est ce que suggèrent Christine Lagarde, la Présidente de la Banque Centrale Européenne, dans son discours du 5 février 2020, ainsi que Jerome Powell, le Président de la Réserve fédérale des États-Unis le 12 avril 2021. Ce dernier déclarait « *Les chances que nous ayons un effondrement qui ressemble de près ou de loin à celui [de 2008] (…) sont très, très faibles. (…) Le monde évolue. Et les risques changent également. Et je dirais que le risque que nous surveillons le plus actuellement est le risque cyber. (…)* ». Dans une enquête sur le risque

systémique menée en 2019 par la Banque d'Angleterre, 61% des participants ont d'ailleurs exprimé leurs inquiétudes quant à l'impact sur le système financier de cyberattaques si elles devaient se matérialiser, plaçant ainsi le risque cyber devant le risque géopolitique et le risque d'un ralentissement économique mondial.

Bien que les considérations de risque cyber aient été progressivement intégrées dans le cadre de la gouvernance et de la gestion des risques des autorités monétaires et financières (Kashyap et Wetherilt, 2019), la disponibilité d'outils de suivi du risque cyber reste cependant très limitée (une exception est l'étude de Jamilov, Rey et Tahoun., 2021, qui propose une mise en perspective historique de l'évolution de ce risque à travers le monde et au sein des principaux secteurs d'activité économique).

Un outil de suivi quotidien et en temps réel du risque cyber

Dans Lhuissier et Tripier (2021), nous construisons un nouvel indicateur du risque cyber depuis 2011. La finalité de l'indicateur est de permettre un suivi à haute fréquence, quotidien, du risque cyber et une analyse des différents secteurs de l'économie concernés.

Le risque cyber se définit comme la combinaison de la probabilité de survenance des incidents cyber (incidents malveillants ou non qui mettent en péril la cybersécurité d'un système d'information ou enfreignent les procédures et règles de sécurité) et de leur impact. Pour en mesurer son évolution, nous avons calculé la part des messages consacrés au risque cyber sur le réseau social Twitter depuis dix ans. Plus précisément, notre indicateur reflète la fréquence de tweets, émis par les utilisateurs anglophones, qui contiennent le duo de mots suivant : « cyber » et « risque », « attaque », ou « menace ». Les avantages de notre méthodologie sont multiples : elle permet 1) d'englober tous les évènements qui se sont réalisés au niveau mondial et ont donné lieu à des échanges en anglais sur ce réseau social, 2) de pondérer l'importance d'un évènement par rapport à un autre (un évènement majeur se verra naturellement attribuer plus de tweets qu'un évènement dérisoire), et 3) de suivre de manière quotidienne et en temps réel le développement du risque cyber. Il faut néanmoins garder à l'esprit les limites de cet indicateur. Il ne couvre que les acteurs de l'économie présent sur ce réseau, et qui plus est anglophones. De plus, nous ne mesurons que la fréquence de l'occurrence des mots clefs liés au risque cyber, sans analyser le contenu des messages ni les interactions des émetteurs de ces messages.

Le graphique 1 affiche l'évolution de notre indicateur de risque cyber de janvier 2011 à août 2021. La plus forte occurrence des messages liés à la cybersécurité sur Twitter que nous mesurons a eu lieu en mai 2017 lors de l'attaque WannaCry, un logiciel malveillant qui a frappé des centaines de milliers d'ordinateurs dans des centaines de pays. L'évènement majeur le plus récent que nous identifions est l'attaque en mai 2021 de la société Colonial Pipeline (gestionnaire d'un oléoduc entre Houston et New York) qui a eu des répercussions politiques importantes (dont la réunion sur la cybersécurité organisée le 25 août dernier par le Président Joe Biden).

Certains évènements se répercutent sur les marchés financiers. À titre d'exemple, en décembre 2020, le piratage de SolarWinds, éditeur de logiciels de gestion informatique et fournisseur d'agences fédérales et de sociétés américaines, a paralysé jusqu'à 18 000 clients et plus d'une centaine de sociétés américaines. L'action SolarWinds Corp a chuté d'environ

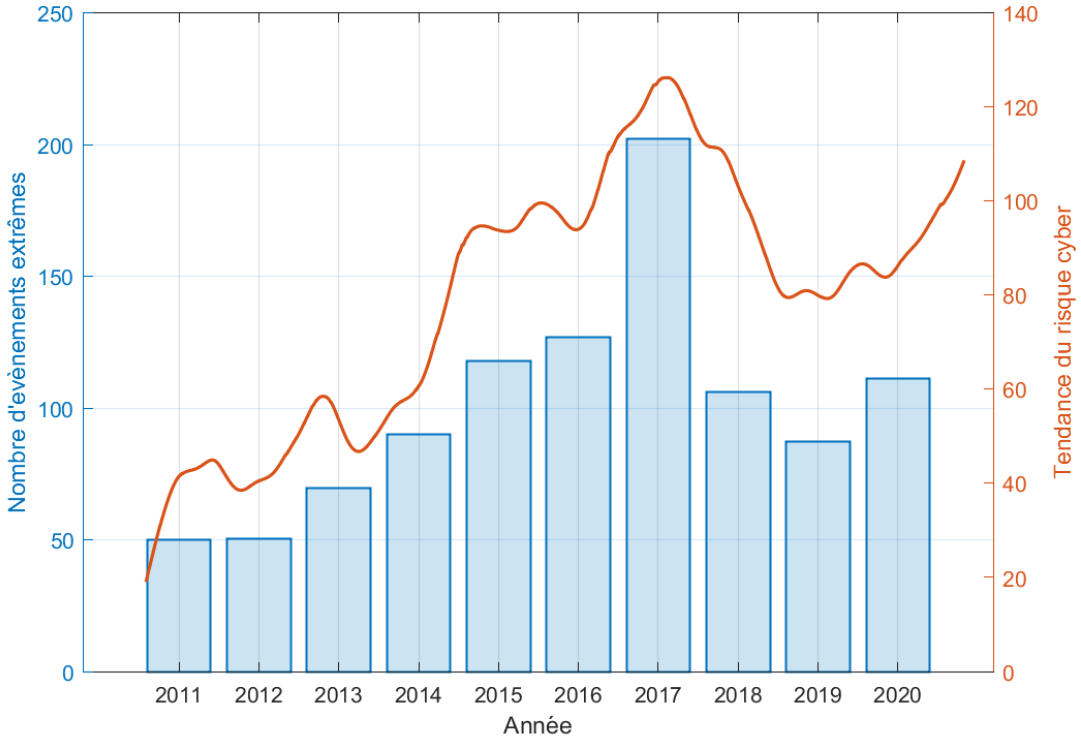
40% en seulement quelques jours à la suite de l'attaque. Bien que ses effets n'aient pas provoqué d'incidents majeurs dans le secteur financier, on pourrait tout à fait imaginer qu'un tel scénario se produise dans le futur. La très forte digitalisation et interconnexion du secteur financier en fait un secteur particulièrement exposé au risque systémique, c'est-à-dire que les conséquences de l'incident cyber se transmettent bien au-delà de l'entité initialement impactée causant des dommages au système économique et financier dans son ensemble.

Une décomposition tendance-cycle du risque cyber

L'indicateur fournit une mesure du risque cyber à haute fréquence, quotidienne. Cependant, il ne permet pas d'avoir une vision claire de ses tendances. Afin de mieux appréhender la tendance du risque cyber, le graphique 2 affiche le nombre d'évènements extrêmes par année, définis ici comme les valeurs de l'indice les plus élevées (top 5%), ainsi que la tendance à long-terme de l'indice purgée des évènements extrêmes.

Entre 2011 et 2017, le nombre d'évènements extrêmes augmente de manière constante, avant de chuter en 2018 et 2019, et de rebondir en 2020. Cette évolution du risque cyber s'observe également à travers sa tendance de long terme. En effet, la tendance montre une attention croissante pour la cybersécurité jusqu'en 2017, puis ravivée à partir de 2020 dans le contexte de la crise sanitaire de la COVID-19. Ces évolutions s'expliquent logiquement par l'usage croissant des technologies de l'information et les transformations de l'organisation du travail et de la production, de plus en plus à distance et connectée.

Graphique 2 – Une recrudescence inquiétante du risque cyber depuis la crise sanitaire

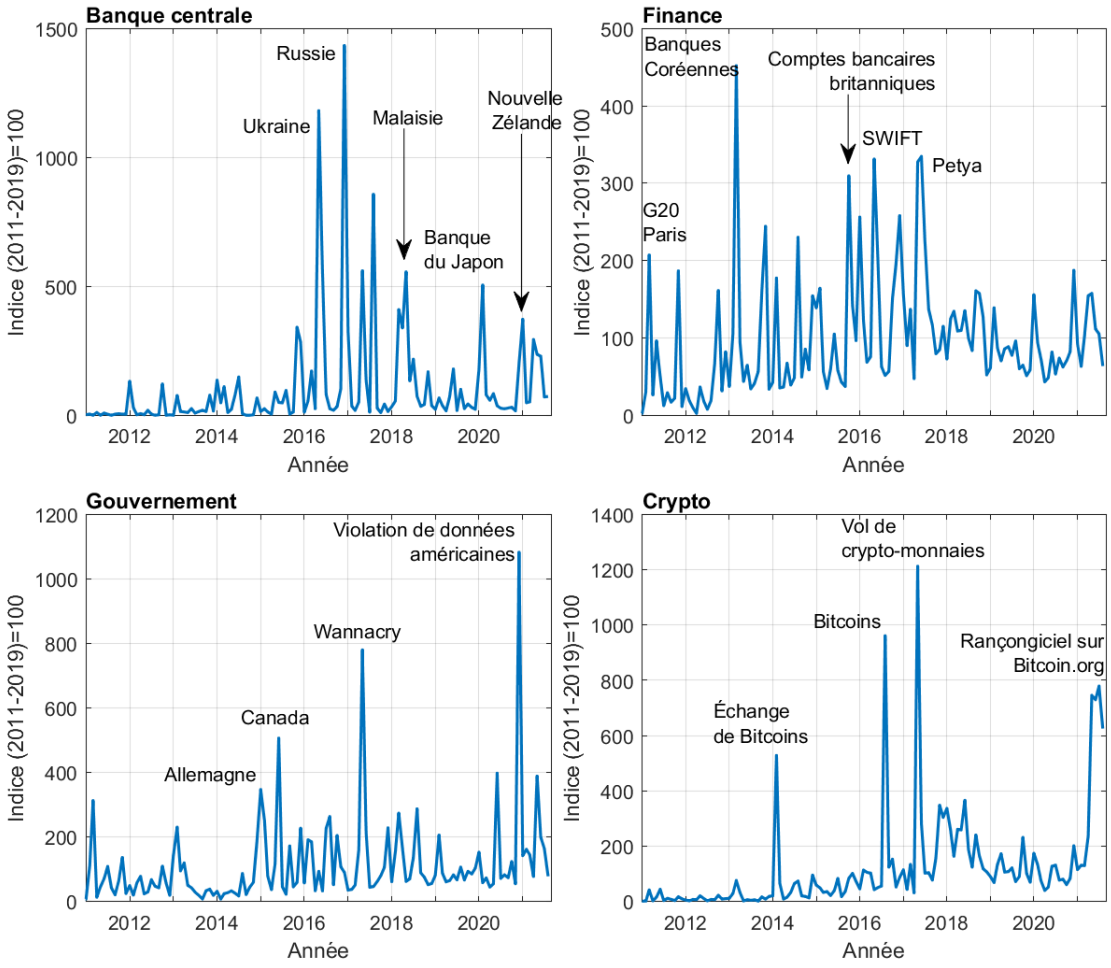


Source : Twitter et calcul des auteurs.

Des indicateurs sectoriels du risque cyber

En complément de notre indicateur de référence, nous développons des indices au niveau des secteurs les plus exposés aux cyber attaques en imposant des critères plus restrictifs lors des recherches de tweets. Par exemple, pour un indice spécifiquement lié au secteur financier, nous recherchons les mots supplémentaires suivants : « banque », « obligation », « marché financier », « pénurie de crédit », « monnaie », « dette », « dividende », « titres », et « finance ».

Graphique 3 – Indicateurs sectoriels du risque cyber



Source : Twitter et calcul des auteurs.

Le graphique 3 présente un exemple de sous-indicateurs étudiés dans notre analyse : banque centrale, finance, agences gouvernementales, et crypto-monnaie. Chacun de ces secteurs sont des cibles populaires pour les cyber criminels comme ils détiennent de nombreuses informations confidentielles et personnelles. À titre d'illustration, le risque cyber auquel sont exposées les banques centrales a atteint son plus haut niveau avec l'attaque de la banque centrale Russe en 2016, où des hackers ont volé plus de 2 milliards de roubles (24 millions d'euros) à partir de comptes de correspondant. Cependant, les pics ne sont pas nécessairement liés à la réalisation de cyber attaques. Par exemple, l'indicateur a

connu une forte progression en janvier 2020 lorsque la Banque du Japon s'inquiéta des risques de cyber-attaques avant le coup d'envoi des Jeux Olympiques. Autre exemple, le risque cyber auquel sont exposés les marchés financiers a connu une progression significative durant des évènements majeurs tels que l'attaque du sommet du G20 à Paris ou celui du réseau SWIFT, ou bien encore le rançongiciel Petya en 2017. Le graphique 3 montre également une recrudescence particulièrement inquiétante du risque cyber concernant les cryptoactifs (cet indicateur est construit en limitant les tweets de notre indicateur de référence à ceux liés aux cryptomonnaies). Les plateformes d'échange de cryptoactifs font effectivement l'objet d'un nombre croissant de cyber attaques (par exemple, la plateforme Bitcoin.org en juillet 2021).

Bien que les attaques informatiques n'aient pas engendré pour l'instant de crise économique et financière globale, certains cyber incidents pourraient toutefois affecter nos économies à l'avenir comme dans les scénarios étudiés par le comité européen du risque systémique (rapport de février 2020). Ainsi, le risque cyber n'est pas seulement un enjeu de sécurité informatique, il est donc important de l'intégrer et l'analyser dans le cadre de surveillance des risques macroéconomiques et financiers.