Document généré le 23 avr. 2024 14:52

Assurances et gestion des risques
Insurance and Risk Management

Quels instruments de couverture pour la gestion du cyber-risque ?

Wissem Ajili

Volume 87, numéro 1-2, juillet 2020

URI : https://id.erudit.org/iderudit/1070752ar
DOI : https://doi.org/10.7202/1070752ar

Aller au sommaire du numéro

Éditeur(s)

Faculté des sciences de l'administration, Université Laval

ISSN

1705-7299 (imprimé)
2371-4913 (numérique)

Découvrir la revue

Citer ce document

Ajili, W. (2020). Quels instruments de couverture pour la gestion du cyber-risque ? *Assurances et gestion des risques / Insurance and Risk Management*, *87*(1-2), 69–99. https://doi.org/10.7202/1070752ar

Résumé de l'article

L'article s'intéresse au cyber-risque en tant que menace émergente pour la stabilité de l'économie mondiale. Aujourd'hui, le paysage des risques tout entier semble subir de profonds changements sous l'effet de la digitalisation. Le défi consiste alors à trouver un compromis entre les avantages escomptés de la numérisation et les risques inhérents aux nouveaux modèles économiques qu'elle impose. Le remodelage de la cartographie des risques mondiaux sous l'effet du cyber-risque impose une réflexion sur la nature de ce risque et ses conséquences, mais nécessite surtout des réponses en matière de couverture. En effet, bien que le marché de la cyber-assurance réagisse à cette nouvelle catégorie de risques, l'offre de cyber-produits demeure en deçà des attentes des acteurs. L'article présente le concept de cyber-risque pour ensuite mettre l'accent sur la question de l'anticipation, de la mesure et de la quantification du cyber-risque. L'article décrit également les progrès accomplis en matière de mise en oeuvre d'un cadre de gestion du cyber-risque, notamment grâce aux travaux de l'Organisation de coopération et de développement économique (OCDE). L'article discute enfin de nouvelles pistes de réflexion pour la couverture du cyber-risque au sein des marchés financiers et l'utilisation des produits dérivés, principalement les titres assurantiels (*Insurance-Linked Securities* ou *ILS)*.

Tous droits réservés © Faculté des sciences de l'administration, Université Laval, 2020

Ce document est protégé par la loi sur le droit d'auteur. L'utilisation des services d'Érudit (y compris la reproduction) est assujettie à sa politique d'utilisation que vous pouvez consulter en ligne.

https://apropos.erudit.org/fr/usagers/politique-dutilisation/

Cet article est diffusé et préservé par Érudit.

Érudit est un consortium interuniversitaire sans but lucratif composé de l'Université de Montréal, l'Université Laval et l'Université du Québec à Montréal. Il a pour mission la promotion et la valorisation de la recherche.

https://www.erudit.org/fr/

Assurances et gestion des risques, Vol. 87 (1-2)
Insurance and Risk Management, Vol. 87 (1-2)

QUELS INSTRUMENTS DE COUVERTURE POUR LA GESTION DU CYBER-RISQUE ?[1]

Wissem AJILI[2]

RÉSUMÉ

L'article s'intéresse au cyber-risque en tant que menace émergente pour la stabilité de l'économie mondiale. Aujourd'hui, le paysage des risques tout entier semble subir de profonds changements sous l'effet de la digitalisation. Le défi consiste alors à trouver un compromis entre les avantages escomptés de la numérisation et les risques inhérents aux nouveaux modèles économiques qu'elle impose. Le remodelage de la cartographie des risques mondiaux sous l'effet du cyber-risque impose une réflexion sur la nature de ce risque et ses conséquences, mais nécessite surtout des réponses en matière de couverture. En effet, bien que le marché de la cyber-assurance réagisse à cette nouvelle catégorie de risques, l'offre de cyber-produits demeure en deçà des attentes des acteurs. L'article présente le concept de cyber-risque pour ensuite mettre l'accent sur la question de l'anticipation, de la mesure et de la quantification du cyber-risque. L'article décrit également les progrès accomplis en matière de mise en œuvre d'un cadre de gestion du cyber-risque, notamment grâce aux travaux de l'Organisation de coopération et de développement économique (OCDE). L'article discute enfin de nouvelles pistes de réflexion pour la couverture du cyber-risque au sein des marchés financiers et l'utilisation des produits dérivés, principalement les titres assurantiels (*Insurance-Linked Securities* ou *ILS)*.

Mots clés : cyber-risque, cartographie des risques, couverture, cyber assurance, produits dérivés, titres assurantiels *ILS*.

JEL classification : G20, G22, G32, M15.

ABSTRACT

This paper focuses on cyber risks as an emerging threat to global economic stability. Today, the whole risk landscape seems to be undergoing profound changes because of digitalization. The main challenge is finding a compromise between the expected benefits of digitalization and the risks inherent to the new

business models it imposes. The rise of cyber risks in global risk mapping certainly requires a reflection on the nature of this risk as well as its extent and consequences, but above all else, hedging responses are required. The cyber-insurance market is responding to this new risk category; however, as an emerging industry, the supply of cyber insurance and reinsurance remains well below the actors' expectations. Undoubtedly, the main difficulties faced by risk managers are those of anticipating, measuring, and quantifying cyber risks. First, the author focuses on the concept of cyber risk, its characteristics and scope, and the sphere of its stakes. Second, the author emphasizes the issues of cyber-risk anticipation, measurement, and quantification. Third, the author describes the progress made in establishing a framework for managing cyber risk, particularly through the work of the Organization for Economic Cooperation and Development. Finally, the author opens a debate on the new lines of thinking for improving cyber-risk hedging through the financial markets and the use of derivatives, mainly insurance-linked securities.

Keywords: cyber risk, risk mapping, risk hedging, cyber insurance, derivatives, insurance-linked securities (*ILS*).

JEL Codes: G20, G22, G32, M15.

INTRODUCTION

La digitalisation de l'économie est porteuse de nouvelles opportunités. En réduisant les asymétries d'information et les coûts de transaction, la numérisation accroît la concurrence sur les marchés, abaisse les prix, favorise l'innovation et augmente *in fine* le bien-être des consommateurs. Toutefois, cette digitalisation n'est pas exempte de nouveaux risques. Les menaces potentielles augmentent, notamment avec le développement de la cybercriminalité et la multiplication des cyber-attaques.

Le défi de la communauté internationale à court et moyen termes consiste à trouver un compromis entre les bienfaits escomptés de la digitalisation des économies et des sociétés et les risques inhérents aux nouveaux modèles économiques qu'elle impose. Aujourd'hui, le paysage tout entier des risques subit de profondes transformations sous l'effet de la digitalisation. L'entrée ascendante du cyber-risque sur la cartographie des risques mondiaux impose, certes, une réflexion sur la nature de ce risque, son étendue et ses conséquences mais nécessite surtout des réponses en matière de gestion et de couverture. En effet, force est de constater que le marché de la cyber-assurance réagit à cette nouvelle catégorie de risques. Toutefois, s'agissant d'une industrie naissante, l'offre de cyber-produits et notamment de cyber-assurance et réassurance reste nettement en deçà des attentes des acteurs. La

difficulté majeure à laquelle se heurtent les cyber-managers est sans doute celle de l'anticipation, de la mesure et de la quantification du cyber-risque.

Cette contribution s'intéresse au cyber-risque d'un point de vue économique et financier. L'objectif est de définir le cyber-risque, de délimiter son périmètre et de recenser les forces et les faiblesses des moyens de couverture existants. Néanmoins, par comparaison aux travaux d'Ajili (2020), l'apport majeur de cet article est de mettre en avant le recours aux produits dérivés, plus précisément aux titres assurantiels (*Insurance-Linked Securities* ou *ILS*), pour la couverture du cyber-risque. En effet, l'analyse du cyber-risque permet d'identifier un comportement d'acteurs analogue à celui adopté en cas de catastrophes naturelles ou de pandémies. La proposition est justifiée par l'intérêt économique de créer une classe d'actifs permettant aux compagnies d'assurance et de réassurance de couvrir un risque qui touche un nombre croissant d'acteurs économiques, tout en assouplissant leur contrainte de fonds propres. La proposition se justifie également dans un contexte où de plus en plus d'investisseurs, principalement institutionnels, sont à la recherche de nouveaux actifs financiers assurant une plus grande diversification de leurs portefeuilles avec des rendements plus stables.

L'article est organisé en cinq sections : la première section présente la notion de cyber-risque, ses caractéristiques, son étendue et la sphère de ses enjeux. La deuxième section s'intéresse à la question de mesure et de quantification du cyber-risque. La troisième section décrit les avancées réalisées pour la mise en place d'un cadre de gestion et de gouvernance du cyber-risque notamment à travers les travaux de l'Organisation de coopération et de développement économique (OCDE). La quatrième section pose la problématique de couverture du cyber-risque, dominée aujourd'hui par le marché de la cyber-assurance. La dernière section se focalise sur la couverture du cyber-risque à travers les produits dérivés, notamment les titres assurantiels (*ILS*).

1. La notion de cyber-risque

1.1. Le cyber-risque, tentative de définition

Sur le plan linguistique, le risque est souvent assimilé à un danger ou à une situation dangereuse. En effet, le risque se définit d'au moins trois manières[3] différentes dans la langue française : (1) possibilité, probabilité d'un fait, d'un évènement considéré comme un mal ou un dommage ;

(2) danger, inconvénient plus au moins probable auquel on est exposé ; (3) fait de s'engager dans une action qui pourrait apporter un avantage mais qui comporte l'éventualité d'un danger. Ainsi, ces différentes définitions, plus ou moins convergentes, témoignent de la difficulté à cerner le concept de risque et à délimiter son champ d'application.

Le risque, au sens large du terme, est un concept au croisement de plusieurs disciplines : l'économie, la finance, les mathématiques, la psychologie, les sciences de l'ingénieur et plus récemment les neurosciences. Le risque est également une notion variable en fonction de son domaine d'application. En finance, le risque signifie la perte financière potentielle qui résulte d'un processus de décision. Pour un assureur, le risque désigne l'indemnisation d'un dommage causé à l'assuré ou à une tierce personne. En statistiques, le risque est la probabilité d'occurrence d'un évènement aléatoire. Pour l'ingénieur, le risque est plutôt un dysfonctionnement ou une erreur dans un procédé ou un processus. Enfin, en médecine, le risque est synonyme de l'apparition d'une pathologie.

À défaut d'une approche unique et universelle du risque, chaque discipline a amélioré son appréhension et sa gestion des risques au fil du temps. À titre indicatif, les financiers identifient et mesurent avec plus ou moins d'aisance plusieurs types de risques comme le risque de marché (risque de change, de taux d'intérêt et de rendement), le risque de crédit, le risque de liquidité et de solvabilité, etc.

Le cyber-risque, en tant que catégorie de risque, ne fait pas exception. Ainsi, le cyber-risque demeure une notion difficile à appréhender et ce, pour diverses raisons. Le cyber-risque est tout d'abord un concept relativement récent et qui ne cesse d'évoluer au fil du temps. Le cyber-risque est également un concept dynamique dont la probabilité d'occurrence et l'intensité d'impact augmentent rapidement. Dans sa conception la plus large, le cyber-risque (ou risque numérique) est le risque qui résulte des incertitudes liées à l'environnement numérique. Ainsi, à la difficulté de définir la notion de risque en tant que telle s'ajoute la difficulté liée aux propriétés intrinsèques de son environnement numérique, à la fois ouvert, interconnecté, mondial et en pleine mutation.

Force est de constater le défaut d'une définition académique du cyber-risque. Néanmoins, l'OCDE, dans sa recommandation (VII.1) de 2015, propose de définir le risque en général comme « *l'effet de l'incertitude sur l'atteinte des objectifs* ». Elle définit ensuite le cyber-risque comme « *une catégorie de risques liée à l'utilisation, au développement, et à la gestion de l'environnement numérique dans le cadre d'une activité quelle qu'elle soit.* »

En conclusion, le cyber-risque désigne tout type de risque résultant des incertitudes liées à l'environnement numérique.

Selon Héon et Parsoire (2017), le cyber-risque couvre six catégories différentes de risques à savoir :

1. Le vol de données : il s'agit du cas le plus fréquent de cyber-risque qui concerne un large panel d'entreprises et d'organisations. Ce risque porte sur les données personnelles (des données personnelles identifiables, des données de santé protégées, des informations de cartes de paiement, des identifiants de connexions comme les mots de passe, etc.) ou sur des informations stratégiques d'entreprises (R&D, F&A, états financiers, propriété intellectuelle, etc.).
2. La cyber-extorsion (*ransomware*) : il s'agit de logiciels malveillants qui pénètrent dans les réseaux informatiques et encryptent toutes les informations disponibles. L'attaquant demande alors une rançon généralement en crypto-devise en échange du décryptage de ces données.
3. La fraude du « *fake CEO* » : dans ce cas, l'attaquant se fait passer pour un membre de la direction puis invite les employés à transférer de l'argent en urgence vers un compte bancaire externe en prétendant qu'il s'agit d'une activité confidentielle comme, par exemple, des démarches en vue d'une fusion ou d'une acquisition.
4. La perturbation d'infrastructures critiques : il s'agit d'interruption ou de dysfonctionnement dans le processus industriel ou commercial sans dommage physique. Ce cyber-risque peut se traduire par l'arrêt ou l'interruption du fonctionnement d'un réseau informatique en le saturant par une grande masse de données.
5. La modification ou le détournement de produits et de services : ce type d'attaque qui se concentre sur les équipements et le matériel communs à plusieurs entreprises (notamment le cas Swift[4]) pourrait constituer le cyber-risque le plus menaçant en matière d'impact. Les attaquants dans ce cas sont plutôt talentueux et organisés, ils agissent par l'intermédiaire de logiciels spécifiques et bien ciblés.
6. Les attaques informatiques donnant lieu à des dommages physiques : ce type de cyber-attaque est également préoccupant dans la mesure où il est présent à chaque fois qu'un appareil est connecté à internet.

L'examen des différentes catégories de cyber-risque permet de distinguer les menaces de nature intentionnelle (actes de malveillance) de celles de nature accidentelle Ainsi, le cyber-risque intentionnel inclut les dommages causés par les cyber-attaques, la fraude liée à l'utilisation abusive des données, la responsabilité née du stockage de données et de leur confidentialité. Le cyber-risque de nature accidentelle couvre quant à lui tous dysfonctionnements pouvant affecter les Systèmes d'information (SI) industriels ou de gestion. Il touche aussi bien les éléments «*hardware*» comme les chaînes de production, les équipements, les câbles, etc. que les éléments «*software*» allant des logiciels, des applications aux sites internet.

L'association des professionnels de la réassurance en France (APREF, 2016) propose une définition causes-conséquences du cyber-risque résumée dans le schéma 1.

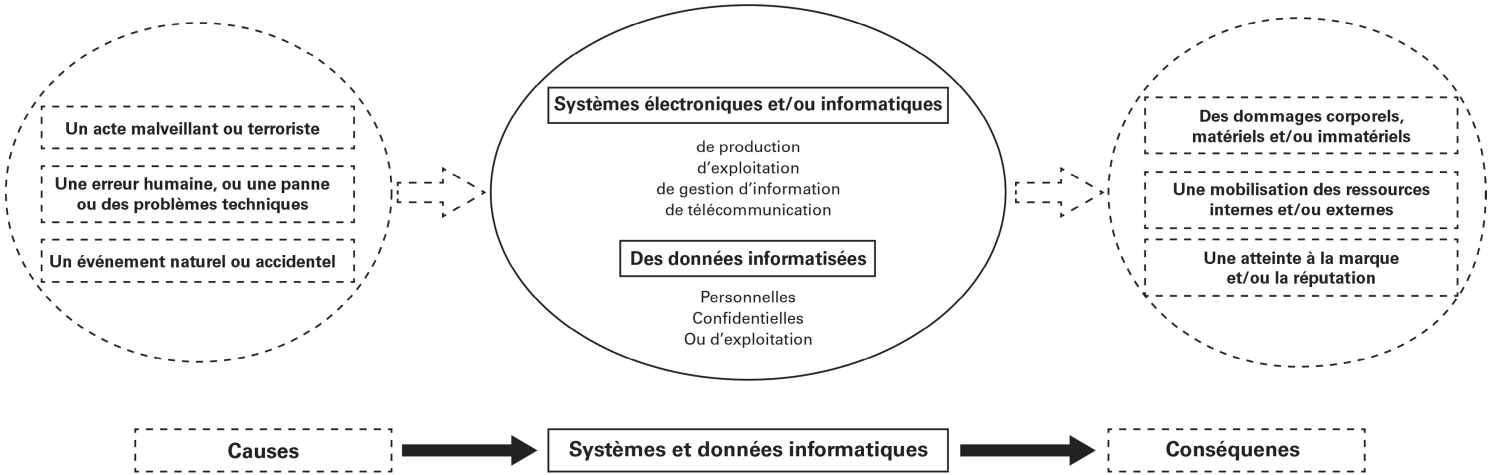
1.2. Le cyber-risque, quelques faits marquants

Le cyber-risque est un risque relativement récent qui a, au plus, trente ans d'existence. Il est révélateur des nouveaux risques du XXIe siècle ; il évolue rapidement et touche les entreprises en affectant la valeur de leurs actifs intangibles (capital intellectuel, réputation, image, brevets, marques, données, etc.)

Le cyber-risque s'est transformé en quelques années, passant d'un risque à caractère opérationnel à une véritable menace pour la stabilité économique et sociale. Aujourd'hui, le cyber-risque bouleverse la cartographie des risques traditionnels et progresse aussi bien en matière de probabilité d'occurrence qu'en matière d'impact potentiel. Le caractère potentiellement systémique du cyber-risque constitue un défi, aussi bien pour les gouvernements, pour les décideurs en matière de politiques nationales que pour les institutions internationales.

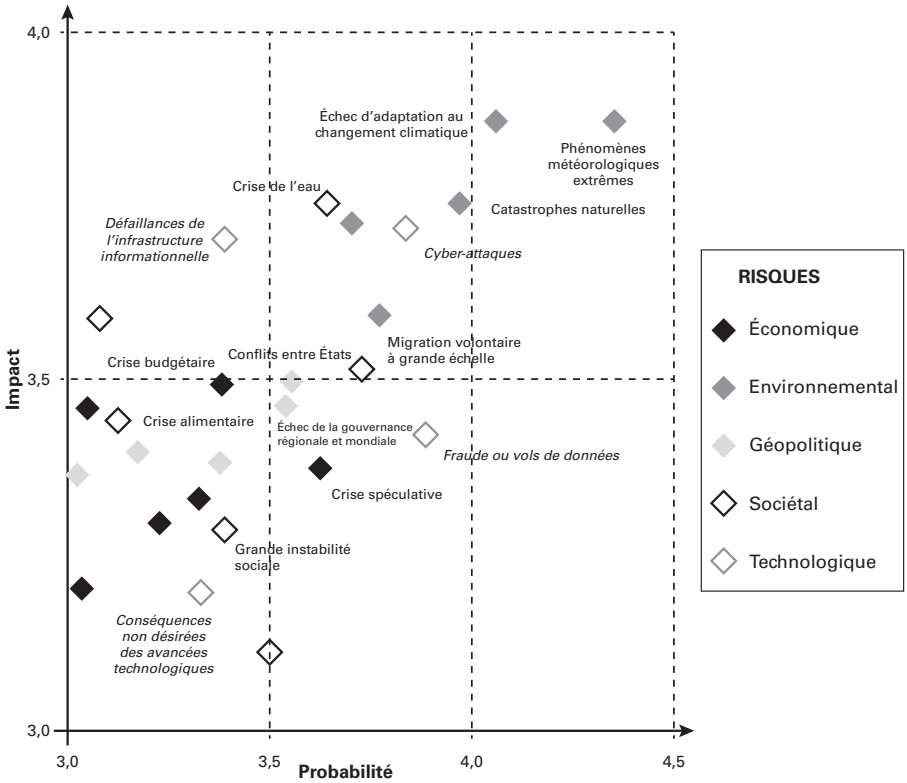
Selon le rapport annuel sur les risques mondiaux du Forum économique mondial (FEM, 2019), le cyber-risque fait partie des dix premiers risques qui menacent le monde en 2019 (voir figure 1). Ainsi, en matière de probabilité d'occurrence, le risque de fraude et de vol de données se trouve en 4e position et les cyber-attaques en 5e position. En matière d'impact potentiel, les cyber-attaques occupent la 7e position et les pannes d'infrastructure informatique critique la 8e position.

SCHÉMA 1 *Une représentation schématique du cyber-risque*



Élaboration de l'auteur d'après l'APREF, 2016, p.16

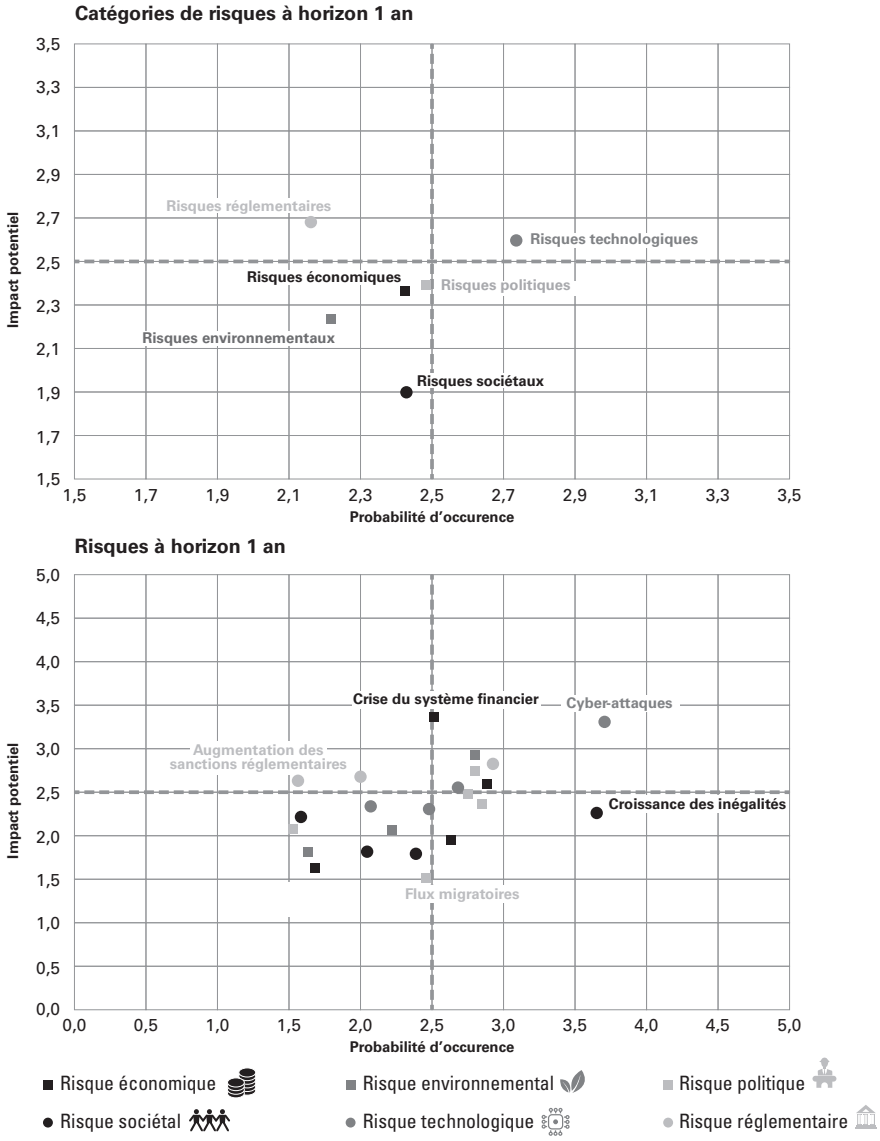
FIGURE 1 *Cartographie des risques mondiaux en 2019*



D'après le FEM, 2019, p. 5

En France, le cyber-risque est perçu par les sociétés d'assurance comme le principal risque émergent. Ainsi, selon le baromètre des risques émergents pour la profession de l'assurance et de la réassurance, établi par la Fédération française de l'assurance (FFA, 2019), le cyber-risque apparaît comme le risque principal auquel les sociétés du secteur font face. Sa probabilité de réalisation est de 3,7/5, pour une intensité potentielle de 3,3/5. Concernant ce baromètre, quatre types de risques technologiques ont été retenus, à savoir la pertinence de l'information et la qualité des données ; les cyber-attaques ; l'inadaptation aux nouvelles technologies et la disruption du secteur (voir figure 2). Parallèlement, les prévisions à l'horizon fin 2022 révèlent que le cyber-risque serait perçu comme le risque majeur auquel ferait face le secteur de l'assurance en France ; avec une probabilité de réalisation supérieure à celle de 2019 soit 4,2/5 et une intensité potentielle plus élevée, soit 4,1/5.

FIGURE 2 *Le baromètre 2019 des risques émergents en France*



D'après la FFA, 2019, p. a5

De son côté, l'Association pour le management des risques et des assurances d'entreprise (AMRAE) confirme cette progression continue du cyber-risque en France. Selon la 5e édition du baromètre du *risk manager* publiée en 2017, le cyber-risque fait désormais partie du top trois des risques pris en compte par les *risk managers*. En 2015, le cyber-risque était classé en 6e position. En deux ans, le cyber-risque a

donc progressé de trois places dans le classement des risques majeurs gérés dans les entreprises françaises. Entre 2015 et 2017, la prise en compte des risques liés à la cyber sécurité est passée de 67% à 79%, celle des risques numériques de 54% à 71%.

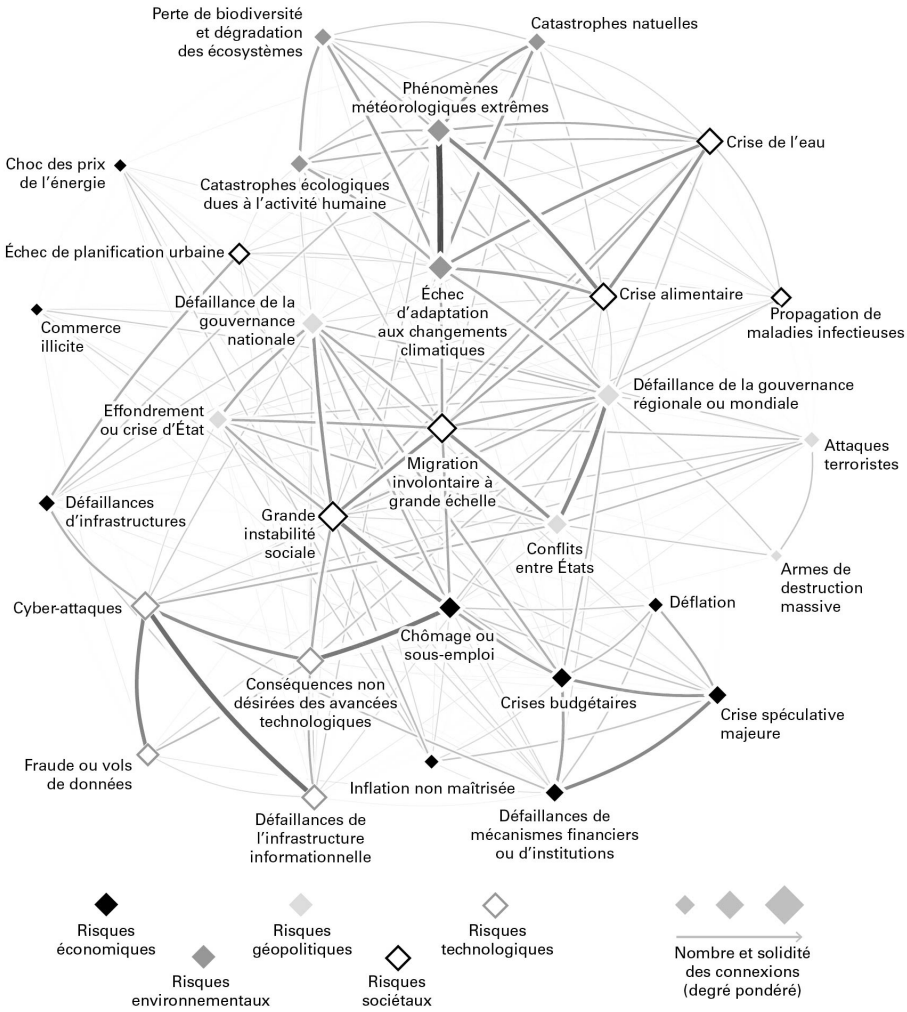
Le cyber-risque pourrait constituer dans les années à venir le risque futur le plus important à gérer par les *risk managers*, notamment pour son caractère potentiellement systémique. Dans son rapport sur l'évolution des risques du système financier français de 2019, la Banque de France considère que la digitalisation s'est traduite par un changement de nature du cyber-risque devenu progressivement plus systémique.

Le caractère potentiellement systémique du cyber-risque signifie qu'il est primordial d'agir de manière concertée et coordonnée à l'échelle mondiale pour gérer ce risque ascendant. Le rapport sur le risque systémique (2010) considère ce dernier comme « *le risque de dégradation brutale de la stabilité financière, provoqué par une rupture dans le fonctionnement des services financiers et répercuté sur l'économie réelle.* » En conséquence, le risque systémique est un risque d'une gravité supérieure puisqu'il est de nature macroéconomique, par opposition aux risques microéconomiques comme le risque de taux ou le risque de défaut. Il peut, à travers l'effet de contagion qu'il implique, entraîner dans son sillon tous les acteurs de l'économie.

À défaut d'une définition précise et consensuelle du risque systémique, ce dernier est souvent appréhendé en matière d'externalités négatives. Par externalités négatives, il est entendu tout impact en l'occurrence négatif que peut avoir le comportement d'un agent économique sur un autre agent économique, sans que le premier ne supporte le préjudice subi par le second.

Le rapport conjoint du FMI-BRI-CSF[5] de 2009 identifie les firmes et les marchés d'une importance systémique, sur la base de trois critères que sont la taille, l'absence de substituabilité et l'interconnexion. Par la taille, il est entendu le volume des services fournis par un acteur ou un groupe d'acteurs. Le critère de la non-substituabilité implique un degré de dépendance relative de tout le système par rapport aux services fournis par le seul acteur ou groupe d'acteurs. Enfin, l'interconnexion est le critère par lequel sont appréciés les liens directs et indirects entre entités qui peuvent faciliter la propagation du risque systémique. La transposition de ces trois critères du secteur financier aux cyber-activités révèle le caractère intrinsèquement systémique du cyber-risque. Les cyber-activités sont non seulement de taille importante et peu substituables mais elles présentent surtout un degré d'interconnexion élevé (voir figure 3).

FIGURE 3 *La carte des interconnexions des risques en 2019*



D'après le FEM, 2019, p. 6

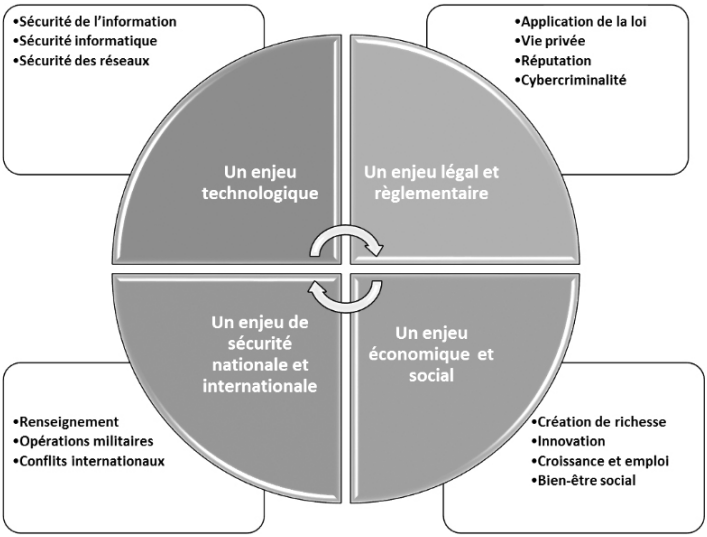
Le cyber-risque se présente aujourd'hui comme un risque systémique, qui se dessine au-delà des frontières géographiques et des limites du temps, et dont les modes de propagation et d'agrégation sont totalement ignorés. Le risque systémique est intrinsèquement un enjeu d'ordre international qui implique des réponses internationales, concertées et coordonnées. L'expérience accumulée à travers l'histoire des crises financières systémiques renseigne sur la nécessité de mise en place de mécanismes de supervision, de régulation et de prévention des évènements systémiques.

1.3. Le cyber-risque, étendue et sphère des enjeux

Le cyber-risque est un risque de nature multiple et complexe qui concerne tous les acteurs de l'économie. Ainsi, le cyber-risque menace aussi bien les gouvernements que les entreprises privées, les organismes publics, les organisations à but non lucratif, les institutions nationales et internationales et les citoyens.

La sphère des enjeux du cyber-risque couvre aujourd'hui quatre domaines : (1) l'enjeu technologique, qui porte sur la sécurité de l'information, la sécurité informatique et la sécurité des réseaux ; (2) l'enjeu légal et règlementaire, en rapport avec l'application de la loi, le respect de la vie privée, la protection de la réputation et la cybercriminalité ; (3) l'enjeu économique et social, relatif à la croissance économique, la création des emplois, le bien-être social ; et enfin (4) l'enjeu de sécurité nationale et internationale qui concerne le renseignement, les opérations militaires et la gestion des conflits internationaux (voir schéma 2 pour une synthèse des différents enjeux du cyber-risque).

SCHÉMA 2 *Les différents enjeux du cyber-risque*



Élaboration de l'auteur publié dans Ajili, W. 2020, p.19

En conclusion de cette première section consacrée à la notion du cyber-risque, et à défaut d'une définition universelle et consensuelle, nous proposons d'identifier les caractéristiques principales du cyber-risque. Il s'agit tout d'abord d'un risque lié à l'incertitude de l'environnement numérique au sens large du terme, dans la mesure où cette

incertitude concerne le matériel, les logiciels mais également les ressources humaines. Le cyber-risque affecte la sécurité (disponibilité, intégrité et confidentialité) des données. Le cyber-risque est de nature économique et sociale et pourrait se traduire par des pertes financières, de compétitivité, de confiance, par une atteinte à l'image ou à la notoriété, etc. C'est, pour finir, un risque qui a des effets négatifs (tout effet positif est qualifié d'opportunité) et qui peut avoir des externalités négatives sur les économies et les sociétés.

2. Le cyber-risque, mesure et quantification

La modélisation du cyber-risque constitue l'un des défis majeurs pour la gestion et la couverture de ce risque. Sans la compréhension de la genèse du cyber-risque et des mécanismes de sa propagation et d'agrégation, il est difficile d'anticiper les cybermenaces et de gérer leurs conséquences.

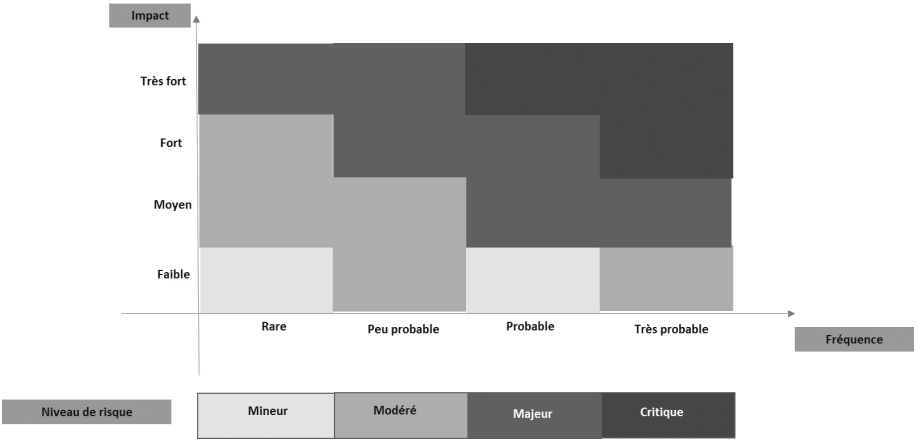
Paradoxalement, à l'ère du *Big Data*, les données relatives aux cyber-attaques demeurent peu exploitables. Non seulement ces données sont relativement rares mais, lorsqu'elles existent, leur pouvoir de prédictibilité est faible, les données historiques étant peu représentatives du futur.

2.1. La cartographie des risques, avantages et limites

Le risque se mesure assez souvent selon deux critères : la probabilité d'occurrence (ou la fréquence) et l'intensité (ou l'impact). Ainsi, une répartition spatiale des différents risques en fonction de ces deux critères est possible. Il s'agit d'une cartographie des risques dite fréquence/impact (voir schéma 3). Cette cartographie des risques permet de définir différents niveaux de risque : le risque mineur, modéré, majeur et critique, chaque niveau de risque étant représenté sur la cartographie par une zone différente.

Toutefois, si la cartographie des risques s'avère utile pour appréhender des risques hétérogènes et les classer en fonction de leur degré de criticité, son caractère général et son approche globale réduisent sa portée. Aujourd'hui, comme souligné dans la première section de l'article, le cyber-risque est de plus en plus pris en considération dans la cartographie des risques mondiaux, avec une probabilité de réalisation croissante et un impact potentiel grandissant. Néanmoins, l'établissement de ces cartographies demeure le résultat d'enquêtes menées souvent

SCHÉMA 3 *Une cartographie des risques fréquence/impact*



D'après Pierandrei, L., 2019 p. 88

auprès de professionnels. En conséquence, ces cartographies doivent être lues et interprétées avec prudence, en tenant compte de plusieurs biais méthodologiques (méthode de collecte de l'information, représentativité de l'échantillon, taille de l'échantillon, etc.) et cognitifs (perception, mémoire, appréciation, etc.) qui peuvent réduire leur significativité. En définitive, ces cartographies traduisent une appréciation plus ou moins subjective de la criticité du cyber-risque à un instant donné, assez souvent établie sur la base d'un échantillon de professionnels.

Le recours aux enquêtes pour l'appréciation du cyber-risque, en dépit de leurs limites, s'explique en partie par la méconnaissance de ce risque mais également par le défaut de méthodes de quantification opérationnelles.

2.2. Le paradoxe de l'indisponibilité des données relatives au cyber-risque à l'ère du *Big Data*

Force est d'admettre que le cyber-risque est difficilement quantifiable. L'OCDE (2017) souligne l'existence de deux problèmes pour la quantification du cyber-risque ; l'indisponibilité des données d'une part, la difficulté à modéliser le cyber-risque d'autre part. En effet, les agents économiques, en général, et les entreprises, en particulier, communiquent peu sur les cyber-attaques. S'agissant d'un risque en pleine mutation, l'expérience accumulée est peu représentative du futur, ce qui rend la tâche de modélisation de ce risque difficile.

Le problème de quantification du cyber-risque au sein même des entreprises peut également s'expliquer par le cloisonnement organisationnel et fonctionnel entre les structures des technologies de l'information (IT) et les structures en charge de la gestion des risques. Ainsi, parmi les préalables à la mesure et à la quantification du cyber-risque, figure la restructuration des entreprises et des organisations touchant de nombreuses fonctions : les *risk managers*, les responsables opérationnels, les responsables financiers, l'IT, etc.

La quantification du cyber-risque n'est pas une finalité en soi. Elle constitue une condition nécessaire mais non suffisante pour couvrir ce risque. En effet, si aujourd'hui le cyber-risque est difficilement assurable, trois raisons cumulatives l'expliquent : (1) il s'agit d'un risque difficilement quantifiable ; (2) le cyber-risque n'est pas parfaitement aléatoire comparé au risque politique ou au risque de guerre ; et (3) le cyber-risque est potentiellement systémique, l'inter connectivité et l'externalisation des services informatiques conférant au cyber-risque ce caractère systémique.

3. Pour un cadre de gestion du cyber-risque

La gestion du cyber-risque a évolué, jusqu'à récemment, dans la sphère purement informatique et technique. Avec la prise de conscience croissante de l'impact économique et financier de cette catégorie de risque, le sujet est devenu l'une des problématiques du *risk management*. D'un risque opérationnel géré au quotidien, le cyber-risque est devenu progressivement l'un des risques stratégiques pouvant affecter la capacité des organisations à définir, orienter et mettre en œuvre leurs stratégies.

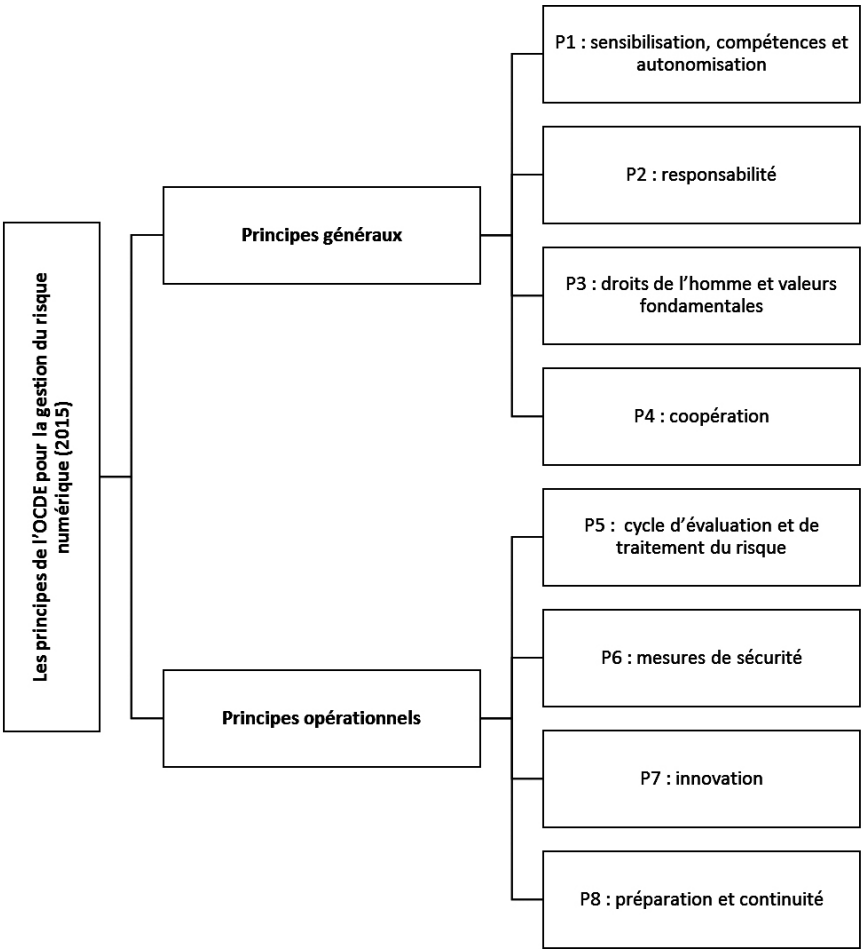
3.1. Les travaux de l'OCDE pour la mise en place d'un cadre de gestion du cyber-risque

La recommandation (VII.2) de l'OCDE (2015), relative à la gestion du risque de sécurité numérique pour la prospérité économique et sociale, soutient la mise en œuvre d'une approche cyclique et flexible de gestion du cyber-risque. Elle décrit le processus de gestion du cyber-risque comme « *l'ensemble des mesures coordonnées intra et/ou inter organisations prises pour maîtriser le risque de sécurité numérique tout en maximisant les opportunités. Elle fait partie intégrante du processus décisionnel et s'inscrit dans un cadre global de gestion du risque qui pèse sur les activités économiques et sociales.* »

La démarche préconisée par l'OCDE pour la gestion du cyber-risque se fonde sur une approche économique d'optimisation. En effet, la gestion du cyber-risque a pour objectif de réduire le cyber-risque à un niveau acceptable au regard du contexte et des objectifs, sans pour autant l'éliminer définitivement. Selon l'OCDE (2015), l'objectif de gestion du cyber-risque consiste à « *définir le niveau de risque acceptable et s'assurer que les mesures de sécurité numérique sont adaptées et proportionnées au risque.* »

En parallèle, l'OCDE (2015) a développé un cadre pour la gestion du cyber-risque basé sur quatre principes généraux et quatre principes opérationnels (voir schéma 4).

SCHÉMA 4 *Les principes de l'OCDE pour la gestion du cyber-risque*

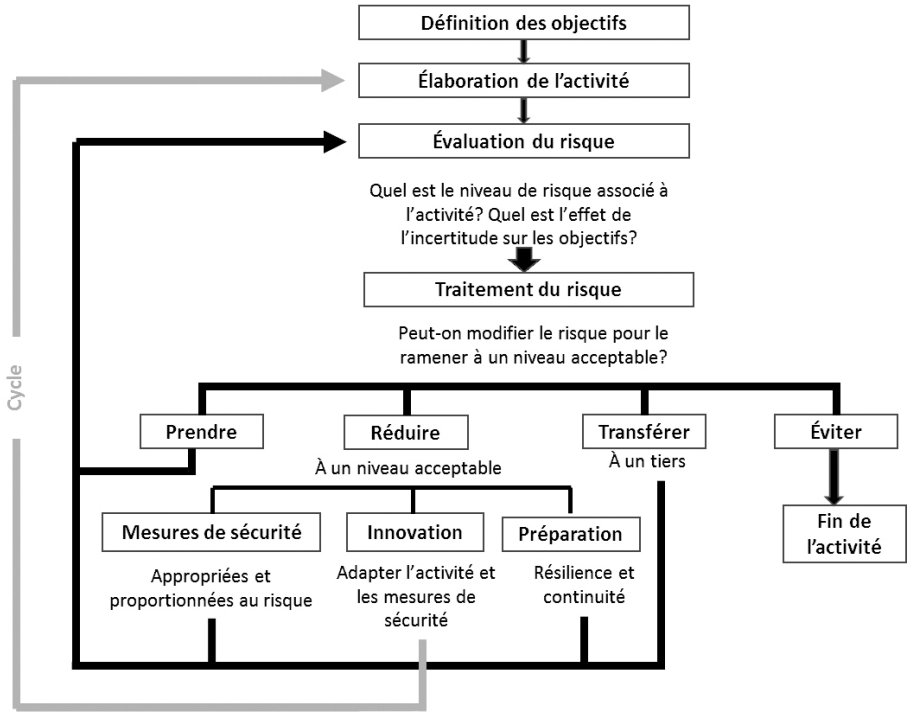


Élaboré par l'auteur d'après l'OCDE, 2015

L'ensemble des principes, notamment ceux à caractère opérationnel, ont abouti à l'élaboration d'un processus de gestion du cyber-risque par l'OCDE (voir schéma 5). Ce processus se base sur l'évaluation du cyber-risque associé à toute activité économique et sociale puis sur son traitement, c'est-à-dire l'étude des moyens possibles pour le ramener à un niveau tolérable ou acceptable. Le traitement du risque doit aboutir à l'une des quatre situations suivantes :

1. la prise en charge du cyber-risque par l'entité (auto-assurance) ;
2. la réduction du cyber-risque à un niveau acceptable à travers la mise en place de mesures de sécurité, l'innovation en adaptant l'activité aux mesures de sécurité, la préparation et la résilience ;
3. le transfert du cyber-risque à un tiers (assurance et réassurance) ;
4. le contournement du risque en mettant fin à l'activité, lorsque le cyber-risque est jugé très important.

SCHÉMA 5 *Le processus de gestion du cyber-risque*



D'après l'OCDE, 2015

3.2. Le *Cybersecurity Act* de 2019

Le *Cybersecurity Act* désigne le règlement européen (UE) 2019/881 du 17 avril 2019, publié au Journal Officiel de l'UE le 7 juin 2019. Le *Cybersecurity Act* vise le renforcement de la règlementation européenne relative à la cyber sécurité. Il s'agit d'un acte juridique européen obligatoire et de portée générale. Les États membres de l'Union européenne (UE) sont tenus d'appliquer toutes les dispositions du règlement entré en vigueur à partir de juin 2019. Néanmoins, les États membres disposent d'un délai de deux ans pour la mise en conformité avec les différentes règlementations nationales.

Le *Cybersecurity Act* a pour objectif la définition d'une stratégie européenne pour la sécurité numérique à travers (1) l'adoption d'un mandat permanent de l'agence européenne pour la cyber sécurité (ENISA) et (2) la définition d'un cadre européen de certification de cyber sécurité pour les produits, les services et les processus des Technologies de l'information et de la communication (TIC).

En ce qui concerne le mandat de l'ENISA, le *Cybersecurity Act* prévoit le renforcement et la consolidation des missions de l'agence dans plusieurs domaines tels que le développement des politiques européennes, le soutien des États membres dans les processus d'élaboration et de mise en œuvre des politiques nationales, l'expertise, la coopération, etc.

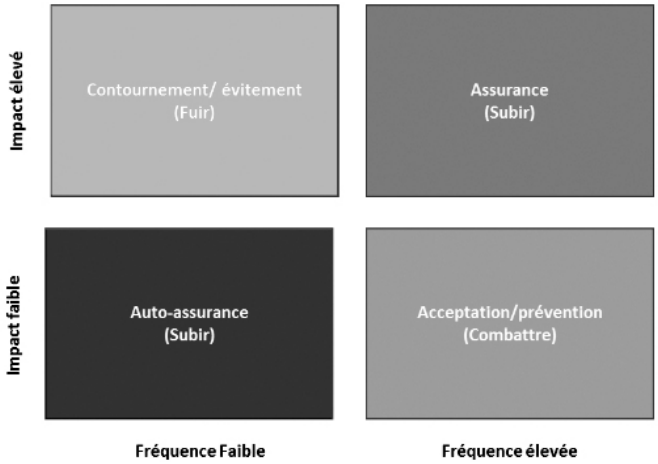
Parallèlement, le *Cybersecurity Act* vise la mise en place d'un cadre européen de certification de la cyber sécurité en unifiant les méthodes d'évaluation et les niveaux d'assurance de certification de cyber sécurité. Le règlement fixe les exigences auxquelles doivent répondre les organismes d'évaluation délivrant les certificats de cyber sécurité. Il définit plus précisément trois différents niveaux d'assurance : (1) un niveau d'assurance « élémentaire » qui cible les produits, services et processus TIC non critiques ; (2) un niveau d'assurance « substantiel » qui vise un risque médian et (3) un niveau d'assurance « élevé » qui porte sur des risques d'attaques menées par des acteurs avec des ressources et des compétences importantes.

4. La couverture du cyber-risque

Pour la gestion du cyber-risque, quatre stratégies différentes sont possibles. Ces stratégies peuvent être définies par le biais d'une matrice fréquence/impact. En effet, selon une approche coût-bénéfice, toute stratégie devrait être bâtie sur le principe d'un coût de gestion du

risque ne devant pas excéder la perte potentielle qu'il est censé couvrir (voir schéma 6). Lorsque la fréquence et l'impact du cyber-risque sont tous deux relativement élevés, l'assurance devient la meilleure solution pour la gestion dudit risque. L'évolution de la place du cyber-risque sur la cartographie des risques explique ainsi le recours accru au marché de l'assurance au cours des dernières années.

SCHÉMA 6 *Les stratégies de gestion du cyber-risque*



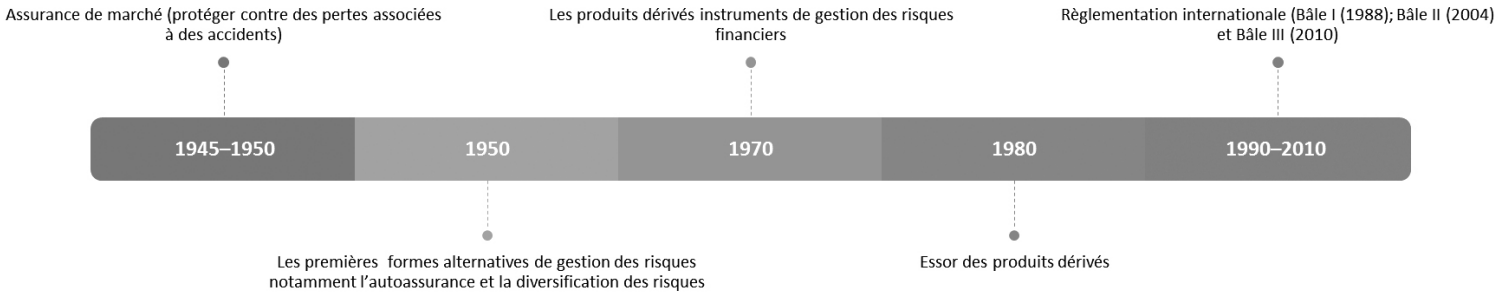
Élaboration de l'auteur d'après Pierandrei, L., 2019, p. 58

Néanmoins, la lecture historique de l'évolution de la gestion des risques (voir schéma 7) révèle que du moment où les acteurs perçoivent la cyber-assurance comme coûteuse et incomplète, des couvertures alternatives, à travers la diversification et l'auto-assurance, gagnent du terrain pour céder ensuite la place aux produits dérivés. Aujourd'hui, le vrai défi est celui du développement de produits dérivés pour la couverture du cyber-risque.

4.1. Le marché de la cyber-assurance

La couverture du cyber-risque est assurée pour sa grande majorité par le marché de la cyber-assurance. L'assurance est l'opération par laquelle une personne, l'assuré, se fait promettre pour lui ou pour un tiers, une prestation de la part de l'assureur en cas de réalisation d'un risque, moyennant le paiement de primes. L'assurance repose sur le principe de la mutualisation du risque. En effet, l'assureur collecte pour une même catégorie de risques l'ensemble des primes versées par les assurés afin de pouvoir indemniser les sinistrés.

SCHÉMA 7 *La gestion des risques, quelques repères historiques*



Élaboration de l'auteur publié dans Ajili, W. 2020, p. 20

Les chiffres relatifs à la taille du marché de la cyber-assurance sont peu précis et se basent sur des estimations. La valeur des primes souscrites en 2015 est estimée à 2,5 billions d'USD. Les prévisions pour 2020 s'établissent entre 9 et 10 billions d'USD. Par ailleurs, le marché américain représente à lui seul 90% du marché mondial. Le marché de la cyber-assurance, notamment européen, est naissant et relativement peu structuré. Toutefois, ce marché en construction demeure à fort potentiel ; selon certaines estimations, le marché européen devrait atteindre une taille comprise entre 0,5 et 1 billion d'USD en primes souscrites à l'horizon de 2020 (SCOR, 2017).

Sur le plan opérationnel, un cadre pour l'analyse des cyber-risques et des couvertures proposées par les assureurs existe en France. Mis en place en 2014 au sein de la commission système d'information de l'AMRAE, un groupe travail « Cyber Assurance » a établi une « matrice type » d'analyse des cyber-risques et des couvertures d'assurance au sein d'une entreprise. La matrice est structurée autour de cinq étapes :

- Étape 1 – Identification des risques : établissement d'une liste indicative des cyber-risques potentiels auxquels l'entreprise est exposée.
- Étape 2 – Évaluation des impacts : il s'agit de recenser la typologie des impacts des différents risques aussi bien sur l'assuré que sur les tiers et d'établir une évaluation financière des différents risques identifiés.
- Étape 3 – Traitements en place : cette étape consiste à déterminer les mesures mises en place pour la gestion et la réduction des risques recensés, puis à identifier les mesures de protection et de prévention élaborées par l'entreprise.
- Étape 4 – Polices d'assurance actuelles : il s'agit de décrire les réponses apportées par les différentes polices d'assurance souscrites par l'entreprise (responsabilité civile, dommage aux biens et/ou pertes financières, fraude, cyber, etc.).
- Étape 5 – Résultats actuels et besoins d'adaptation : lors de cette dernière étape, les *risk managers* sont incités à se poser la question de l'efficacité des couvertures existantes et à détecter le cas échéant les limites et les insuffisances du système en place.

La matrice simplifiée de gestion des cyber-risques définit les cyber-risques sur la base deux critères : les faits générateurs dommageables (atteintes aux données, extorsion, fraude, entrave au fonctionnement, avec et sans dommage physique, etc.) et les conséquences dommageables (actifs corporels, actifs financiers, frais informatiques, e-réputation, etc.) (voir figure 4).

FIGURE 4 *Matrice simplifiée pour l'analyse des cyber-risques*

		Faits générateurs dommageables									
		Atteintes aux données sur attaques	Atteintes aux données sur erreur	Extorsion	Fraude	Entrave au fonctionnement sans dommage physique	Manipulation du produit ou du service client sur attaque	Manipulation du produit ou du service client sur erreur	Dommage matériel suite à attaque	Dommage matériel suite à erreur	Relais d'attaque
Conséquences dommageables	Actifs corporels	SO	SO	DAB	Fraude	SO	SO	SO	DAB	DAB	SO
	Actifs financiers	SO	SO	Cyber	Fraude	SO	SO	SO	SO	SO	SO
	Perte d'exploitation	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
	Frais informatiques	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
	Protection des données personnelles confidentielles	Cyber	Cyber	Cyber	SO	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
	E-réputation/ Communication	Cyber	Cyber	Cyber	SO	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
	Protection juridique	Cyber	Cyber	Cyber	Fraude	Cyber	Cyber	Cyber	Cyber	Cyber	Cyber
	Responsabilité civile (dommages aux tiers)	RC	RC	RC	RC	RC	RC	RC	RC	RC	RC
	Amendes et pénalités	Cyber		Cyber	Fraude	Cyber	Cyber		Cyber	Cyber	Cyber

DAB : Police Dommage aux Biens ; RC : Police Responsabilité Civile ; Cyber : Police Cyber ; SO : Sans Objet

D'après l'IRT, 2016, p. 38

4.2. La couverture du cyber-risque, limites et insuffisances

Force est d'admettre que le cyber-risque est un risque réel qui ne cesse de croître avec la digitalisation de l'économie et la numérisation des sociétés. Toutefois, le cyber-risque demeure mal appréhendé. La structure des organisations, basée souvent sur un cloisonnement des services techniques et ceux en charge de la gestion des risques, rend l'objectif de mise en place d'une approche globale de gestion des risques intégrant le cyber-risque de plus en plus difficile à atteindre. L'état des lieux de la couverture du cyber-risque met en évidence l'existence des problèmes de définition et d'identification des cyber-risques, aussi bien sur le plan théorique que parmi les professionnels. Néanmoins, la principale limite demeure celle de la mesure et de la quantification du cyber-risque. Le manque de données chiffrées, publiques comme privées, le défaut de métriques et *a fortiori* de modèles économiques fiables permettant d'estimer le coût économique des cyber-risques, limitent énormément le potentiel de développement d'instruments et d'outils de couverture. Cette limite s'est accentuée par le manque de données chiffrées relatives au coût économique et financier des cyber-risques. En parallèle, le marché de la cyber-assurance demeure naissant et peu mature, notamment en Europe, et les possibilités de réassurance sont très limitées.

La difficulté à gérer et couvrir le cyber-risque résulte en partie de sa dimension internationale et de son caractère intrinsèquement systémique. Face à un risque qui franchit les frontières géographiques, les lois et les règlementations nationales, la réponse ne peut être qu'internationale. Il est à noter qu'en novembre 2015, le G7 a mis en place le *Cyber Expert Group* (CEG) dont l'objectif est l'indentification des principaux risques en matière de cyber sécurité portant sur le secteur financier et la proposition d'actions à conduire dans ce domaine. Le rapport de la Banque de France sur l'évolution des risques du système financier français (Banque de France, 2019) soutient que la gestion efficace du cyber-risque nécessite une meilleure coopération entre les acteurs, au plan international à trois niveaux différents : (1) la règlementation de la cyber sécurité et sa supervision ; (2) la classification des cyber-incidents et le partage de l'information ; et (3) la préparation de la gestion opérationnelle des crises avec la conduite d'exercice de cyber-résilience.

4.3. Pour une meilleure couverture du cyber-risque, quelques pistes de réflexion

Parmi les pistes à creuser pour une meilleure couverture du cyber-risque figure celle du développement d'une logique financière et économique pour l'évaluation du cyber-risque qui dépasse les analyses techniques utilisées jusqu'à présent. Toutefois, il est au préalable primordial de mettre en place des approches opérationnelles permettant aux *risk managers* une meilleure appropriation du cyber-risque. Si la cyber-assurance est considérée aujourd'hui comme une solution optimale pour les entreprises, c'est parce que le cyber-risque est perçu comme résiduel en comparaison aux investissements requis pour une gestion active de ce risque. Néanmoins, d'autres solutions alternatives pourraient exister, (1) la gestion en interne du cyber-risque (auto-assurance ou *self-financing*) ; (2) la gestion syndiquée par l'intermédiaire d'un *pool* d'assurances ; (3) le transfert du cyber-risque au marché financier.

5. Les *ILS* pour la couverture du cyber-risque

Cette dernière section envisage les *ILS* comme l'instrument de couverture potentiel le plus adapté au cyber-risque. En effet, parmi les produits dérivés tels que les contrats à terme, les *swaps* ou les options,

les *ILS* semblent constituer une réponse optimale aux besoins de couverture du cyber-risque formulés notamment par les compagnies d'assurance et de réassurance.

5.1. Les produits dérivés et la couverture du cyber-risque

Historiquement, les produits dérivés ont vu le jour durant la bulle des tulipes dans les années 1630. Ainsi les premiers contrats *futures* avaient porté sur les matières premières. Dans les années 1970, l'utilisation des produits dérivés comme instruments de gestion des risques a débuté avec des actifs sous-jacents standards comme les actions, les taux de change et les taux d'intérêt. Au cours des années 1980, une nouvelle étape a été franchie par l'introduction des premiers contrats dérivés sur indice. La décennie 1990 a connu l'apparition de produits dérivés pour la couverture des risques climatiques et de défaut. Les innovations des ingénieurs financiers ne se sont pas limitées aux seuls actifs sous-jacents standards. Certains contrats portent aujourd'hui sur l'inflation, le chômage ou encore la volatilité des marchés. En définitive, tout ce qui est objectivement mesurable peut servir de support à des contrats dérivés (Capelle-Blancard, 2009). Ainsi les années 2020 pourraient être la décennie des produits dérivés destinés à la couverture du cyber-risque.

Les produits dérivés sont des instruments financiers qui dépendent d'un actif sous-jacent (matières premières, actions, taux de change, taux d'intérêt, indice, etc.). Ils peuvent être basiques ou complexes, fermes ou optionnels, négociés sur un marché de gré à gré (*Over-The-Counter*, OTC) ou sur des marchés organisés. Les produits dérivés sont également des contrats qui permettent le transfert de risque entre agents économiques en assurant l'échange de flux financiers en fonction de l'évolution de la valeur de l'actif sous-jacent.

Les produits dérivés assurent ainsi trois types d'opérations : (1) la couverture, ou *hedging* en anglais, qui consiste à se protéger contre les fluctuations défavorables du prix de l'actif sous-jacent ; (2) la spéculation qui se base sur la formulation d'anticipation de la part des agents économiques en prenant des positions avec un effet de levier ; et (3) l'arbitrage qui consiste à réaliser un profit sans risque résultant d'une incohérence de prix sur les marchés financiers.

Les produits dérivés peuvent être classés en trois grandes familles, (1) les contrats à terme, (2) les *swaps* et (3) les options. Le contrat à terme est défini comme un engagement ferme et définitif entre deux

parties de livrer, pour l'une, et de recevoir, pour l'autre, une certaine quantité d'actif sous-jacent à une date d'échéance, à des conditions définies à l'avance. Le *swap* est quant à lui un produit dérivé financier. Il s'agit également d'un engagement ferme entre deux parties visant à échanger un flux financier contre un autre flux financier. Enfin, l'option est un contrat établi entre un acheteur et un vendeur. L'acheteur de l'option obtient le droit et non l'obligation d'acheter ou de vendre, selon le cas, un actif sous-jacent à un prix fixé d'avance à ou jusqu'à une date d'échéance, moyennant le versement d'une prime.

Le tableau 1 ci-après résume les caractéristiques des différentes catégories de produits dérivés ainsi que les principales dates de lancement de ces produits (Dionne, 2013).

TABLEAU 1 *Les principales catégories de produits dérivés*

CONTRATS	MARCHÉS	PRINCIPAUX PRODUITS
Forward	OTC	Forward devises – FRA
Future	Organisé	Foreign currency futures (1972)
Swap	OTC	Currency swaps (1970), Cross Currency interest rates swaps (1982), Credit default swaps CDS (1994)
Option	OTC ou organisé	Equity options (1973), Over-The-Counter currency options (1979), Equity index options (1983), Interest rate caps/floors (1983), Swaptions (1983), Path-dependent options : Asian, lookback etc. (1987), Captions/ Floortions (1993)

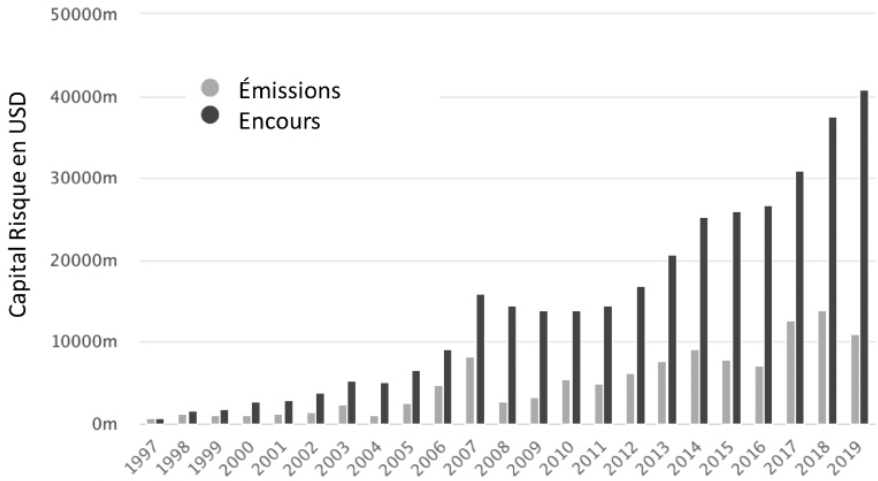
Élaboration de l'auteur

5.2. Le choix des *ILS* pour la couverture du cyber-risque

Pour la couverture du cyber-risque via les marchés financiers, la réflexion devrait être orientée vers les *ILS*. Les *ILS* sont des titres permettant de transférer le risque de catastrophes naturelles des compagnies d'assurance et de réassurance vers les investisseurs, *via* les marchés financiers. Ainsi, les investisseurs prennent en charge les pertes liées aux catastrophes naturelles à la place des compagnies d'assurance moyennant le paiement d'une prime de risque. Le marché des *ILS* a vu le jour au milieu des années 1990, par suite de catastrophes naturelles récurrentes comme les ouragans, les tremblements de terre, les tempêtes ou encore les incendies. Certains auteurs dont notamment Loubergé, Kellezi & Gilli, (1999) ; Scherer, (2000) et Bouriaux & MacMinn, (2009) se sont intéressés au fonctionnement des *ILS* ainsi qu'à leurs avantages et limites.

Au cours des deux dernières décennies, le marché des *ILS* n'a cessé de se développer (voir figure 5). Il attire des investisseurs tels que les fonds de pension, les compagnies d'assurance et de réassurance, les banques, les gestionnaires d'actifs et des fonds alternatifs, tous à la recherche d'avantages que génère une diversification de leurs portefeuilles d'actifs. Plus spécifiquement, les *ILS* sont attrayants car ils représentent un potentiel de rendement intéressant.

FIGURE 5 *Les émissions et encours des obligations catastrophes et des ILS*



www.Artemis.bm Deal Directory

Le produit le plus utilisé sur le marché des *ILS* est l'obligation pour risque de catastrophe, le *Cat Bond*. Le *Cat Bond* est une obligation de courte durée, mais à haut rendement. Elle n'est remboursée au souscripteur qu'en cas de non-réalisation d'un ou plusieurs sinistres prédéfinis avec précision (seuils en matière de puissance, magnitude, zone géographique couverte, etc.). Par conséquent, le *Cat Bond* présente l'inconvénient pour le souscripteur d'une perte totale du nominal. Le montant souscrit est généralement placé par l'émetteur en obligations d'État.

Du côté des émetteurs, les *ILS* permettent aux compagnies d'assurance un arbitrage entre le coût de réassurance et le taux d'intérêt. Les *ILS* permettent également aux compagnies de réassurance d'assouplir leur contrainte de fonds propres.

Du côté des souscripteurs (investisseurs), les *ILS* présentent l'atout considérable d'une faible corrélation avec les autres classes d'actifs financiers. La probabilité de réalisation d'un évènement naturel comme un orage n'est nullement influencée par le niveau des taux d'intérêt, (Scherer, 2000). En effet, les *ILS* sont exposés à des risques totalement indépendants des cycles économiques, des évolutions des taux de change, des taux d'intérêt ou des prix de matières premières. L'intégration des *ILS* dans un portefeuille d'actifs permet d'en réduire la volatilité et d'améliorer la stabilité des rendements.

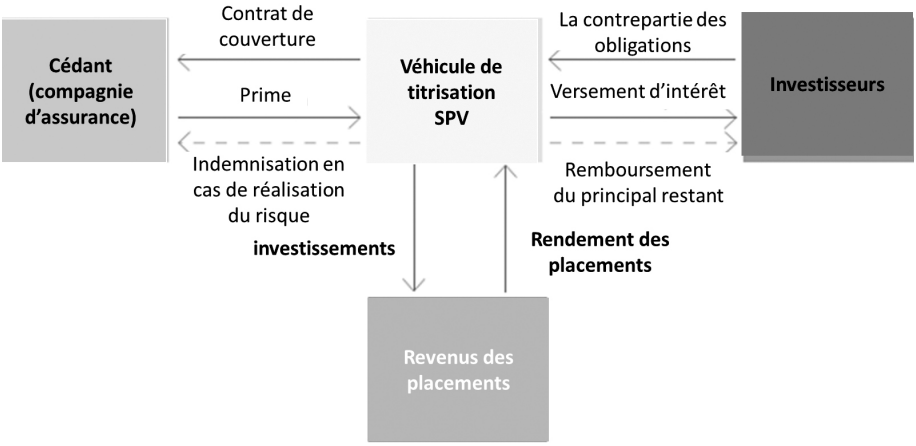
Les *Pondemic Bonds*, émis sous l'égide de la banque mondiale avec le soutien de l'Organisation mondiale de la santé (OMS), constituent également un cas d'obligation assurantielle (ou *ILS*) indexée sur un risque de pandémie (virus Ébola, sida, grippes aviaires, etc.). Les *Pondemic Bonds* fonctionnent comme les *ILS* à quelques différences près. Les souscripteurs de ces obligations pandémiques perçoivent un coupon mais risquent de perdre le principal si les conditions préétablies d'un évènement donné sont réunies. Ainsi, les souscripteurs ne sont pas rémunérés sur la base de la qualité de signature de l'émetteur de ces titres mais par référence à la probabilité de réalisation de l'évènement catastrophe. Par comparaison aux autres types d'*ILS*, les *Pondemic Bonds* n'ont pas été conçus pour faire face aux conséquences financières postérieures à un événement catastrophe, mais plutôt dans une logique préventive. Les *Pondemic Bonds* ont pour objectif de limiter l'effet de propagation de la pandémie. Néanmoins, le succès des *Pondemic Bonds* reste mitigé. Les critiques portent notamment sur (1) les conditions relativement restrictives pour le déclenchement du mécanisme (la vitesse de propagation de la pandémie, le nombre de décès confirmés, la pandémie franchissant les frontières nationales, etc.) ; (2) les conditions financières généralement plus favorables aux souscripteurs aux dépens des bénéficiaires du mécanisme ; (3) enfin, sur le plan éthique, tirer profit d'un investissement dans les catastrophes humanitaires et de santé est difficilement acceptable.

Le cyber-risque tel que présenté au niveau de la première section se prête bien à une couverture *via* les marchés financiers mais à travers une catégorie bien précise de produits dérivés à savoir les obligations assurantielles ou les *ILS*.

En effet, un *ILS* est un instrument financier dont la valeur faciale dépend de la réalisation ou non d'un risque assurable. Les premiers *ILS* structurés, les *Cat bonds,* avaient la forme d'une obligation à taux variable et portaient sur le risque d'une catastrophe naturelle. Le *cat bond* est émis par un véhicule de titrisation (en anglais *Special Purpose Vehicule ou SPV*). Celui-ci est engagé en vertu d'un contrat de

couverture à indemniser le cédant, en contrepartie d'une prime, en cas de réalisation de catastrophe naturelle. La transposition de ce schéma de fonctionnement dans le cadre de la couverture du cyber-risque est parfaitement possible. Le cédant ne serait autre qu'un agent économique (entreprise, banque, société d'assurance ou autres) qui transfèrerait son cyber-risque à une entité financière Ad hoc, le véhicule de titrisation, moyennant le payement d'une prime. Le véhicule de titrisation émettrait sur les marchés financiers des *ILS* (*Cyber-bonds*). Les fonds reçus lors de l'émission des *cyber-bonds* seront conservés par le véhicule de titrisation et constitueraient le collatéral du contrat de couverture. Les *cyber-bonds* seraient remboursables *in fine*. Leur valeur de remboursement serait égale au nominal déduction faite des versements effectués par le véhicule de titrisation dans le cadre de la couverture cyber (voir figure 6).

FIGURE 6 *Représentation schématique du mode de fonctionnement des Cat bonds*



D'après Swiss Re Capital Market, 2011, p. 9

Dans le cas des *cat bonds*, le risque de catastrophes naturelles fait l'objet d'une modélisation détaillée par des sociétés indépendantes. L'approche repose sur un processus en trois étapes (Scherer, 2000) : (1) la constitution d'une base de données des phénomènes de catastrophes naturelles passés et la détermination de leurs probabilités de reproduction dans le futur ; (2) l'estimation des pertes associées à chaque évènement pour les différents portefeuilles assurés ; et (3) l'évaluation de l'impact de ces pertes sur les contrats d'assurance et de réassurance et *in fine* sur la valeur des *cat bonds*. Ces derniers sont par ailleurs soumis à la notation des agences de rating.

Aujourd'hui, il serait parfaitement envisageable de constituer une base de données des cyber-attaques et d'estimer grâce à des modèles stochastiques leurs probabilités de réalisation dans le futur. Une meilleure communication de la part des agents économiques sur les dégâts matériels occasionnés faciliterait la quantification de leur impact financier direct et indirect et *in fine* la valorisation (le *pricing*) des cyber-bonds.

En résumé, le choix des *ILS* pour la couverture du cyber-risque a pour avantage (1) d'atténuer le caractère systémique du cyber-risque en le décorrélant des cycles économiques et des autres risques financiers et opérationnels ; (2) d'orienter les modèles de quantification du cyber-risque vers des approches probabilistes, ce qui permet de contourner le problème de mesure du cyber-risque sur le plan économique ; (3) d'améliorer la résilience des acteurs économiques vis-à-vis du cyber-risque et d'assurer *in fine* une certaine stabilité économique et financière ; et (4) de développer une catégorie d'actifs financiers aux externalités positives sur la volatilité des marchés et en matière de stabilité de rendement.

6. Conclusion

Cet article s'intéresse au cyber-risque en tant que menace montante pour la stabilité de l'économie mondiale. Étant donné sa nature potentiellement systémique, le cyber-risque évolue au-delà des frontières géographiques et touche tous les acteurs de l'économie internationale : firmes multinationales, gouvernements, institutions financières, entreprises et individus. En dépit d'une prise de conscience croissante des enjeux de cette nouvelle catégorie de risque, sa couverture est loin d'être systématique. Les premières réponses sont de nature assurantielle. Néanmoins, le marché de la cyber-assurance demeure peu développé, notamment en Europe. Pour dynamiser cette industrie naissante, la proposition de titres assurantiels, notamment les *ILS*, sur le marché des dérivés serait de nature à diversifier les instruments de couverture du cyber-risque et à soulager la contrainte de fonds propres des compagnies d'assurance et de réassurance. Du côté des marchés financiers, l'introduction de cette classe d'actifs, caractérisée par leur décorrélation par rapport aux cycles financiers et aux évolutions des actifs traditionnels, aurait pour effet d'augmenter la stabilité des rendements en améliorant la diversification des différents portefeuilles.

7. Références bibliographiques

[1] Ajili, W. (2020). Les cyber-risques : nature, étendue et moyens de couverture. *Droit & Patrimoine, (*298), 17-20.

[2] AMRAE. (2017). *Le Baromètre du Risk Manager* (5ème éd.).

[3] AMRAE. (2015). Cyber risques : Outil d'aide à l'analyse et au traitement assurantiel. *Cahiers techniques*.

[4] APREF. (2016). *Étude sur les «cyber risques» et leur (ré)assurabilité*. 1-66.

[5] Association Française des Marchés Financiers. (2017). Cyber risques : la finance en alerte. *L'info AMAFI*, (130).

[6] Banque de France. (2019). *Évaluation des risques du système financier français.*

[7] Bouriaux, S. & MacMinn, R. (2009). Securitization of Catastrophe Risk : New Developments in Insurance-Linked Securities and Derivatives, *Journal of Insurance Issues*, Vol. 32, N°.1 (SPRING 2009), p. 1-34

[8] Capelle-Blancard, G. (2009). Les marchés dérivés sont-ils dangereux? *Revue Économique*, Vol. 60 (2009/1), p. 157-171.

[9] Dionne, G. (2013). Gestion des risques : histoire, définition et critique, CIRRELT-2013-04, Janvier 2013/ https://www.cirrelt.ca/documentstravail/cirrelt-2013-04.pdf

[10] Fédération Française de l'assurance. (2019). *Baromètre 2019 des risques émergents pour la profession de l'assurance et de la réassurance.* https://www.ffa-assurance.fr/sites/default/files/files/2019/02/20190206_-_barometre_2019_des_risques_emergents.pdf

[11] Héon, S. & Parsoire, D. (2017). La couverture du cyber-risque. *Revue d'économie financière*, *2*(126), 169-182.

[12] Institut de Recherche Technologique (IRT). (2016). *La maîtrise du Risque Cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance.* 1-69.

[13] Lepetit, J.F. (2010). Rapport sur le risque systémique. *La documentation française.*

[14] Loubergé, H., Kellezi, E. & Gilli, M. (1999). Using Catastrophe-Linked Securities to Diversify Insurance Risk : A Financial Analysis of Cat Bonds, *Journal of Insurance Issues*, Vol. 22, N°. 2 (FALL 1999). p.125-146

[15] OCDE. (2015). *Gestion du risque numérique pour la prospérité économique et sociale : Recommandations de l'OCDE et document d'accompagnement*. Paris : Éditions OCDE.

[16] OCDE. (2017). *Enhancing the role of insurance in cyber risk management*. Paris : Éditions OCDE.

[17] Pierandrei, L. (2019). Risk Management. (2ème éd.). Paris, France : Dunod.

[18] Règlement (UE) 2019/881 du Parlement européen et du Conseil du 17 avril 2019 (J.O. 7 juin 2019).

[19] Scherer, A. (2000). La titrisation des risques d'assurance : le marché des « insurance linked securities » (ils), *Revue d'économie financière*, N° 59, LA TITRISATION (2000), p.135-146

[20] SCOR. (2017). *Cyber risk on the rise : from intangible threat to tangible (re)insurance solutions*.

[21] Swiss Re Capital Market (2011). The fundamentals of insurance-linked security : Transforming insurance risk into transparent and tradable capital market products, September 2011. https://www.swissre.com/our-business/alternative-capital-partners/ils-the-fundamentals-of-insurance-linked-securities.html

[22] World Economic Forum. (2019). *The Global Risks Report 2019* (14ème ed.).

NOTES

1. Une version réduite de cet article a été publiée dans la revue Droit & Patrimoine N°298 – Janvier 2020 sous l'intitulé « les cyber-risques : nature, étendue et moyens de couverture », p.17-20.

2. Wissem AJILI –ESLSCA Paris – Business School – France & Université de Carthage – ISG de Bizerte – Tunisie : ajiliouissem@yahoo.fr (0033621426530)

3. Définitions tirées du dictionnaire Larousse.

4. Le réseau d'interconnexion bancaire internationale appelé Swift (*Society for Worldwide Interbank Financial Telecommunication*) a fait l'objet d'attaques de cybercriminalité, en 2016. Les attaques ont tout d'abord ciblé la banque centrale du Bangladesh au mois de février et l'opération s'est soldée par le détournement de 81 millions de dollars. Au cours de la même année, les attaquants ont réussi à compromettre le fonctionnement de certains autres systèmes bancaires locaux dont notamment celui de la banque centrale des Philippines à travers un malware qui dissimule les traces de paiements frauduleux sur les bases de données. Les attaques se sont arrêtées fin avril de la même année avec le renforcement des mesures de sécurité du réseau SWIFT.

5. FMI-BRI-CSF = Fonds monétaire international-Banque des règlements internationaux et Conseil de la stabilité financière.