Cyber-assurance : nouveaux modèles pour quantifier l'impact économique des risques numériques

Olivier LOPEZ*
Florence PICARD**

La révolution numérique a apporté de profondes transformations dans la plupart des secteurs économiques. Celles-ci ont modifié la cartographie des risques encourus par les entreprises, notamment les risques informatiques. En quelques années, le *cyber risk* est apparu comme l'une des menaces principales pesant sur les entreprises, comme l'indique notamment le rapport du ministère de l'Intérieur sur le sujet[1]. La mise à disposition de produits d'assurance directement liés au risque cyber contribue à doter le secteur industriel et économique de contre-mesures. La cyber-sécurité physique, chargée de prévenir ou de limiter les dégâts causés aux systèmes d'information, est complétée par un éventail de garanties qui viennent apporter réparations financières, conseils et parfois mesures d'accompagnement des victimes – de la part des assureurs. Puisque aucun système ne peut être considéré comme totalement imperméable aux attaques et aux défaillances, il faut donc considérer cette protection économique comme un outil essentiel de la cyber-défense.

* Co-porteur du projet « Cyber-insurance: actuarial modeling » (Fondation du Risque, Fonds AXA pour la Recherche, AXA GRM, Ensae), Sorbonne Université. Contact : olivier.lopez0@upmc.fr.
** Membre du Directoire, Fondation du Risque ; membre du Comité de direction, ILB ; responsable du groupe de travail Cyber Risk, Institut des actuaires. Contact : florencepicard@aol.com.

Les assureurs doivent appréhender ce nouveau contexte pour offrir aux entreprises les couvertures dont elles ont besoin. Néanmoins l'évaluation de ce risque nouveau et sa tarification nécessitent de nouvelles méthodes pour quantifier l'impact économique du risque : d'une part, le manque de recul ne permet pas de disposer d'une expérience suffisante et, d'autre part, la collecte des données statistiques est particulièrement délicate dans ce domaine en constante évolution. Cette évolution est technologique, mais elle est aussi comportementale. Dans cet écosystème en constante redéfinition, *hackers*, usagers et acteurs de la protection modifient sans cesse leurs pratiques, tandis que leur conscience même du risque évolue. Ces changements dans la nature comme dans la perception de la menace brouillent les analyses. Dans cet article, nous présenterons tout d'abord le contexte du cyber-risque et l'importance des bonnes pratiques des cibles et victimes face au risque. Ces comportements, variés et changeants d'un acteur à l'autre, nous conduiront ensuite à interroger le modèle même de l'assurance cyber, et des difficultés méthodologiques qu'il doit résoudre. Enfin, nous insisterons notamment sur l'importance des données et de leur analyse critique, en tant qu'élément vital de la quantification du risque.

CYBER RISK : DE NOUVEAUX RISQUES ENGENDRÉS PAR LES NOUVELLES TECHNOLOGIES

L'explosion des *data*, la généralisation des objets connectés (par exemple, les smartphones) et la puissance des algorithmes aptes à traiter les données permettent de grands progrès, notamment dans le domaine de la santé.

Mais, comme toute nouvelle technologie dans l'histoire de l'humanité, les technologies numériques présentent aussi des dangers à la hauteur des avantages qu'elles peuvent apporter à la société.

Ces risques sont d'origine immatérielle, agissant via du code informatique, et pas de façon physique. Mais leurs conséquences sont matérielles, voire corporelles, et leur coût peut être extrêmement élevé. Dans un rapport de Cyence et Lloyd's of London[2], il a ainsi été estimé que si un sinistre survenait chez un prestataire de *cloud*, le coût de l'attaque se situerait dans une fourchette de 15 Md$ à 121 Md$, avec une perte moyenne estimée à 53 Md$.

La menace consiste le plus souvent en une intrusion dans le système informatique. Les attaquants utilisent des failles de sécurité pour pénétrer dans le système et y installer un logiciel malveillant (*malware*) programmé par l'attaquant en fonction de son objectif.

Le *malware* et la méthode d'attaque dépendent de la motivation de l'attaquant : financière, lorsqu'il s'agit de prendre possession des don-

nées pour rançonner l'entreprise ou le particulier (par exemple, le rançongiciel *Wannacry* ; Chen et Bridges, 2017, et Navetta *et al.*, 2017) ; économique et concurrentielle, on espionne ou on commet des actes de malveillances envers un concurrent dans le but d'acquérir un avantage commercial ; politique ou idéologique, comme semble l'indiquer la cyberattaque NotPetya (Fayi, 2018) ou le piratage de l'entreprise canadienne Ashley Madison (Mansfield-Devine, 2015). Les classifications des attaques à partir de la motivation de leurs auteurs (on pourra consulter à ce sujet Uma et Padmavathi, 2013) ne traduisent que partiellement la multiplicité des cas de figure. L'émergence d'un marché du *malware* sur le *darkweb* met la vengeance contre un employeur à porter de clic.

Les modes d'actions de l'infection par le *malware* peuvent être divers.

Le logiciel peut agir dès son introduction dans le système d'information et perturber gravement la production. Les attaques réussies entraînent fréquemment des pertes d'exploitation ; une durée supérieure à une dizaine de jours n'est pas rare (Low, 2017).

Mais il peut aussi rester dormant pendant plusieurs mois et travailler contre l'entreprise à son insu. Les dégâts peuvent, dans un cas comme dans un autre, être irrémédiables.

Les attaques informatiques constituent un marché international, souvent structuré et organisé, animé par des *hackers* compétents et créatifs, qui ont souvent un temps d'avance technologique sur leurs victimes.

Prévention du cyber risk

De multiples exemples ont montré ces dernières années la généralisation de la menace et la nécessité dans tous les secteurs économiques de se mobiliser pour s'en protéger : TV5, les hôpitaux britanniques, Saint-Gobain et la Deutsche Bahn font partie des nombreuses victimes des logiciels malveillants comme WannaCry et Petya (Navetta *et al.*, 2017).

Pour une entreprise, quelle que soit sa taille ou sa localisation, la question n'est plus de savoir si elle va être confrontée au risque cyber car elle l'est déjà et le même virus peut attaquer en même temps une PME française, un organisme d'État en Europe et un grand groupe industriel aux États-Unis.

Le sujet est de s'organiser pour que le jour où le risque se réalisera, il ait le moins d'impact possible sur la vie de l'entreprise.

La prévention et l'anticipation sont essentielles pour parer les attaques, empêcher les virus de pénétrer au cœur du système informatique et limiter l'impact d'une attaque réussie.

C'est l'intérêt des entreprises de mettre tout en œuvre pour la sécurité informatique car ce risque n'est pas seulement financier : une indemnisation ne suffit pas à réparer la perte de confiance des actionnaires (cas de Equifax ; Gressin, 2017), ni l'atteinte à l'image et la fuite des clients, qui peut perdurer des années après l'attaque.

Au moment de la souscription d'un contrat, les assureurs portent une grande attention à la qualité des politiques de sécurité mises en place par l'entreprise : le budget et l'efficacité des dispositifs de sécurité informatique bien sûr, mais aussi les procédures pour l'ensemble du personnel, l'organigramme et la place des RSSI (responsables de la sécurité des systèmes d'information) dans les organisations, l'intérêt porté à la cyber-sécurité par le Comex et le conseil d'administration.

En effet, le risque vient le plus souvent de l'extérieur, mais les failles internes ne sont pas seulement techniques. Le plus souvent, ce sont des erreurs humaines qui ouvrent la porte aux attaquants : arnaques au président, mais aussi messages non sécurisés, mots de passe faibles, etc.

Il est important que l'ensemble du personnel participe à la lutte contre la menace cyber : formation et *training* réguliers sont une démarche de prévention indispensable.

De l'importance de l'organisation interne

La prévention passe aussi par une attention portée aux échanges de données, notamment avec les sous-traitants et à la qualité de leur sécurité informatique, pour éviter des contagions, mais aussi pour répartir les risques en cas d'attaque cyber sur les sous-traitants. Le risque de la *supply chain* doit être analysé globalement car il peut y avoir des solidarités fortes entre ses membres face au risque cyber.

Il convient aussi de prévoir exactement ce que chacun à son poste de travail doit faire en cas d'attaque réussie sur le plan technique, mais il faut aussi prévoir une cellule de crise et une communication adaptée. Le coût des conséquences de l'attaque réussie peut varier du simple au centuple selon les actions menées dans les heures qui suivent l'attaque. À cet égard, TV5 fournit un exemple de réaction technique judicieuse rapide qui a sauvé l'entreprise (Untersinger, 2017).

Concernant les données personnelles, le règlement européen RGPD en vigueur depuis mai 2018 oblige, sous peine de sanction, à informer les clients dans des délais très courts (72 heures), ce qui nécessite d'avoir anticipé et préparé les actions à mener dans une telle situation.

Si l'on veut quantifier la perte économique que peut représenter le cyber-risque sur une entité, nous voyons donc que celle-ci est fortement liée au comportement de la victime potentielle. Une entreprise mal

préparée, ou avec une stratégie de réponse déficiente, se verra infliger une perte conséquente. Construire un système viable d'assurance cyber, c'est donc composer avec cette hétérogénéité des comportements, qui pollue considérablement l'analyse du risque.

C'est cette question de l'analyse du risque que nous allons approfondir à présent. Nous nous attacherons notamment à rappeler un certain nombre de principes mathématiques de l'assurance, avant de mettre en évidence qu'ils se trouvent fragilisés dans le contexte du cyber-risque.

LA MODÉLISATION DU RISQUE POUR L'ASSURANCE CYBER

Le risque cyber est transversal à la technique, la production et l'image. Il ne peut donc être complètement transféré à l'assureur. La couverture financière est bien sûr nécessaire, bien qu'insuffisante.

En général, les contrats de responsabilité et de dommage classiques ne sont pas adaptés à ce risque : ils couvrent les conséquences d'événements générateurs matériels, mais pas de faits générateurs immatériels. La tarification des contrats spécifiques mis en place par les assureurs nécessite de construire tout le nouveau matériel adapté à ce nouveau domaine.

Déterminer le coût d'une garantie d'assurance réside dans la difficulté de surmonter deux problèmes souvent imbriqués : l'inversion du cycle de production et l'asymétrie d'information. Par inversion du cycle de production, on entend que le livrable (ici une indemnisation promise par l'assureur) est inconnu au jour où la garantie est évaluée. Cette indemnisation dépend en effet de la réalisation (incertaine) d'un événement dont la gravité elle-même n'est pas forcément connue, rendant le montant de la prestation lui-même aléatoire. L'asymétrie d'information tient quant à elle au fait que l'assuré dispose d'informations sur son risque qui ne sont pas nécessairement remontées à l'assureur.

L'inversion du cycle de production, qui est décrite plus avant ci-dessous, rend nécessaire l'utilisation de modèles pour prévoir le coût. Ces modèles vont nécessiter des données, afin de juger de leur pertinence et les calibrer. C'est là que l'asymétrie d'information entre en jeu (*infra*), en occultant des informations pertinentes pour le modèle.

Inversion du cycle de production

Le phénomène d'inversion de la chaîne de production n'est pas cantonné au strict champ de l'assurance, de nombreux produits financiers reposent eux aussi sur des mécanismes similaires. Il rend nécessaire la construction de modèles prédictifs. La tarification pure vise ainsi à

déterminer la valeur moyenne du coût de la prestation. Celle-ci, sous des hypothèses standards, se résume à la formule classique « fréquence (ou probabilité) de survenance » multipliée par « coût moyen d'un sinistre » (voir, par exemple, Charpentier et Denuit, 2004). Nous verrons par la suite que cette vision peut être mise à mal dans des cas d'accumulation de sinistres, menace importante dans le champ du cyber. Nous commencerons néanmoins par étudier ce cadre avant d'envisager son extension.

Les modèles prédictifs en tarification pure visent à déterminer ces deux quantités. Le terme tarification pure est néanmoins trompeur. La construction du tarif effectif est en effet la résultante de nombreux facteurs : il intègre les incertitudes de modèles, les coûts de gestion, les impératifs commerciaux et concurrentiels. Plutôt que parler de « tarification pure », il est plus opportun de parler de « scénario central ». Le coût de la garantie quant à lui ne se résume pas à la simple détermination du prix, mais à l'évaluation des provisions à constituer afin d'être en mesure de faire face à des événements qui peuvent dévier fortement de ce scénario central.

Pour quantifier le risque, il faut donc des modèles prédictifs. Et pour construire ces modèles prédictifs, il faut connaître le risque, accumuler de l'information le concernant. L'asymétrie d'information, inhérente au contrat d'assurance, complexifie fortement cette tâche, à plus forte raison dans le cadre d'un risque émergent tel que le cyber-risque.

Asymétrie d'information

L'asymétrie d'information est structurelle dès lors que l'assureur possède une vision collective du risque et que l'assuré dispose d'une connaissance plus précise de sa propre situation face à ce risque (voir, par exemple, Abbring *et al.*, 2003). Par exemple, l'assuré peut savoir si son système d'information est mal sécurisé, ce que l'assureur ignorera s'il n'effectue pas les expertises nécessaires. C'est le rôle du questionnaire, présent dans la souscription de nombreux contrats d'assurance, qui vise à corriger cette asymétrie. L'assuré livre alors des éléments jugés clés par l'assureur pour mieux définir son profil de risque, et s'engage sur la sincérité des informations fournies.

Il s'agit ainsi de lutter contre deux phénomènes classiques que sont l'antisélection et l'aléa moral. L'antisélection tient notamment au fait qu'un assuré est souvent plus exposé au risque concerné qu'un individu (ou qu'une entité dans le cas d'une entreprise) pris au hasard dans la population. La souscription d'un contrat d'assurance répond, chez l'assuré, à une prise de conscience du risque, souvent lié à une fragilité ressentie. L'aléa moral, quant à lui, tient à négliger sa propre protection

face au risque pour la faire supporter par l'assureur via sa garantie. À charge au questionnaire de débusquer les fragilités afin de mettre l'assureur au même niveau d'information et de ne pas déséquilibrer la relation économique entre les deux parties.

Néanmoins, dans le contexte du cyber-risque, cette vision d'un assuré qui en connaîtrait plus sur son risque qu'un assureur n'est pas forcément juste (Kesan *et al.*, 2004). Si les grandes entreprises disposent d'experts capables d'évaluer la robustesse de leur système d'information, les PME et les particuliers peuvent avoir des difficultés à évaluer leur propre état de protection. L'asymétrie d'information doit ici moins être comprise comme le moyen pour l'un des acteurs de tirer le maximum de profit du contrat, mais comme le fait que chacun d'entre eux possède une vision partielle (et différente) du risque, sans nécessairement pouvoir l'exploiter.

Le comportement des assurés a un impact sur la capacité de l'assureur à surmonter ces deux difficultés posées par l'asymétrie d'information. Cet aspect est particulièrement exacerbé dans le contexte du cyber-risque. En effet, les changements de comportement des individus conduisent à recalibrer les modèles, voire à les rendre obsolètes. La nouveauté, dans le contexte du cyber, vient notamment de la célérité de ces changements. Nous allons à présent analyser comment la viabilité même du modèle d'assurance cyber peut être mise en danger par l'absence d'une remontée fluide et rigoureuse des informations sur les sinistres. Celle-ci peut en effet introduire des biais importants dans l'analyse.

LA MISE À MAL DU MODÈLE ÉCONOMIQUE DE L'ASSURANCE

La viabilité économique de l'assurance repose fortement sur une bonne anticipation des risques. Pour anticiper, il faut *a minima* disposer d'une information fiable et robuste. Il faut également que s'opère une mutualisation du risque : les aléas propres à un assuré (qui peut aussi bien n'avoir aucun sinistre sur un exercice, que se voir frappé par des pertes catastrophiques) sont amortis par la masse des assurés constituant le portefeuille. Tout d'abord, nous allons nous attacher à décrire comment le comportement changeant des acteurs du secteur conduit à une perte d'information, qui elle-même peut aboutir à des biais importants dans l'analyse. Ensuite ce constat nous conduira à plaider pour la consolidation des bases de données existantes, en envisageant leur difficile mise en cohérence. Enfin, nous verrons que cette information doit notamment viser à envisager le risque d'accumulation, qui met en péril la mutualisation.

Information cachée

Si l'antisélection et l'aléa moral existent potentiellement, nous souhaitons attirer l'attention sur un phénomène moins connu de perte d'information entre l'assuré et l'assureur, et qui tient au comportement de déclaration de l'assuré.

Le phénomène dit de « *hunger for bonuses* » est bien connu dans le secteur de l'assurance automobile (voir, par exemple, Park *et al.*, 2018). Lors de la survenance d'un sinistre, l'assuré dispose d'un choix : effectuer lui-même les réparations sans avoir recours à son assureur, ou faire jouer la garantie. Dans le second cas, l'indemnisation est en général amputée d'une franchise et, dans le cas de l'assurance automobile, d'une augmentation du niveau de malus, lequel débouche sur une augmentation de la prime. L'assuré effectue donc un calcul économique (qui tient également compte des complexités éventuelles de démarches) qui peut conduire à une non-déclaration. C'est en apparence une bonne nouvelle pour l'assureur, puisque un certain nombre de sinistres (en général de faible montant pour l'assurance automobile) n'auront pas à être indemnisés. En revanche, cette absence de déclaration occasionne une perte d'information pour l'assureur (la fréquence d'occurrence des sinistres de l'assuré est plus élevée que ce que l'assureur affiche).

Mathématiquement, on peut montrer que dans des cas standards, négliger la modélisation de ce phénomène n'a pas d'impact sur le scénario central au niveau de son portefeuille (outre les problèmes statistiques d'estimation de la fréquence et de la sévérité). C'est en revanche lorsqu'il s'agit d'évaluer les déviations par rapport à ce scénario qu'un biais intervient (par des calculs élémentaires, on peut facilement mettre en évidence une mauvaise estimation de la variance).

Ce biais est-il important ? Si, comme dans le cas de l'assurance automobile, l'absence de déclaration ne concerne que les petits sinistres, l'impact sera marginal. En revanche, dans le contexte du cyber-risque, les comportements sont plus complexes. Si les petits sinistres peuvent ne pas être remontés car éventuellement non détectés, les plus importants ne sont pas nécessairement déclarés. C'est notamment la crainte pour la réputation (dont la dégradation a des impacts financiers peu aisés à quantifier) qui remplace celle du malus. Dès lors une part significative des sinistres peut rester inconnue.

Il est important de comprendre que si cette part représente à l'heure actuelle des sinistres non indemnisés, ce ne sera pas nécessairement toujours le cas. Car le comportement des assurés vis-à-vis de la déclaration des sinistres cyber change, à la suite notamment des changements de réglementation et de la banalisation des incidents. Dans ces

conditions, même la détermination du scénario central peut se trouver polluée par cette perte d'information. Il est donc crucial de tenir compte de ce comportement et de son évolution dans la conception des modèles prédictifs.

Une information morcelée à rassembler en respectant la cohérence

Nous l'avons vu, l'information sur un risque encore peu connu est cruciale. Et celle-ci est morcelée entre l'assureur (qui a la vision des sinistres se produisant au sein de son portefeuille), l'assuré (qui dispose d'informations sur son contexte propre). À ces deux acteurs s'ajoutent aussi des tiers, entreprises spécialisées ou organisations d'intérêt public recensant des incidents cyber. La difficulté est alors de réconcilier ces visions de nature différente.

La littérature actuarielle abonde en méthodes permettant cette réconciliation. La théorie de la crédibilité (Bühlmann et Gisler, 2006) permet ainsi de trouver le bon compromis entre une expérience du risque au niveau individuel et une expérience plus macroscopique. Plus généralement, les méthodologies bayésiennes concilient un *a priori* (conçu à partir d'une expérience externe du risque) et l'information que l'on possède sur la population assurée (Déniz *et al.*, 2000).

Ces démarches partent du paradigme suivant : si l'on souhaite analyser le risque d'une population de faible taille (telle qu'un portefeuille d'assurance cyber sur lequel l'historique sera faible, ou sur un individu isolé), toute calibration de modèle sera entachée d'une précision statistique faible. On peut en revanche avoir recours à une population de référence, plus vaste, mieux documentée. L'analyse statistique des propriétés de la population de référence est fiable, mais introduit un biais par rapport à l'objectif initial : le portefeuille d'assurés ne se comporte pas comme la population de référence. Néanmoins on peut supposer des similitudes de comportement entre ces deux populations. L'enjeu méthodologique est alors de trouver le point d'équilibre entre l'analyse provenant du portefeuille (non biaisée, mais peu fiable statistiquement) et celle produite à partir de la référence.

Dans le champ de la cyber-assurance, il apparaît indispensable de se tourner vers ce type d'approche, les assureurs disposant d'une expérience trop faible en interne pour obtenir une vision fiable d'un risque en rapide évolution. En revanche, la détermination d'une population de référence est délicate.

Un certain nombre de bases publiques recensent des événements cyber, mais peu sont celles qui relient un incident cyber à sa sévérité. On trouve en effet des bases de données régulièrement mises à jour sur l'apparition de nouvelles vulnérabilités, sans pour autant que le lien

avec la gravité d'une exploitation de ces failles soit évident à déterminer. La base Privacy Rights Clearinghouse (https ://www.privacyrights.org /data-breaches), développée par une association de sensibilisation aux risques liés à la vie privée basée aux États-Unis, est sans doute ce qui ressemble de plus près à une base de données classique en assurance, puisqu'elle associe une fréquence à une sévérité. Elle est largement étudiée dans la littérature actuarielle sur le cyber-risque (voir notamment Eling et Loperfido, 2017, et Forrest *et al.*, 2016).

Cette base, de même que d'autres bases analogues, comporte d'importants biais liés à sa constitution même. Il est donc possible et sans doute nécessaire d'avoir recours à ces sources d'informations, mais pas sans être particulièrement vigilant à leur structure et à la façon dont elles ont été constituées, comme le mettent en évidence notamment Farkas *et al.* (2019). En effet, les critères de constitution de la base ont fortement évolué dans le temps, et si la base recense des sinistres, elle dit peu de chose sur l'évolution de l'exposition au risque au cours du temps.

Le risque d'accumulation

La fiabilité statistique des bases de données utilisées pour évaluer le risque est essentielle, mais ne permet néanmoins que de cerner des phénomènes déjà observés par le passé, ou dont les dynamiques ont été extrapolées. En particulier, la performance des méthodes basées sur l'inférence statistique suppose une forme d'indépendance entre les observations : parce que les données peuvent être envisagées comme le produit d'expériences répétées et effectuées de façon au moins en partie décorellée, on peut en extraire une information stable. Les modèles prédictifs passent alors remarquablement bien à l'échelle de leur utilisation sur un portefeuille d'assurance où les pertes enregistrées par les assurés entretiennent peu de liens. C'est le principe de la mutualisation : une perte significative sur un contrat sera absorbée par des pertes faibles ou nulles sur la masse d'autres contrats. L'approche « fréquence-coût » est taillée pour ce cadre.

En revanche, le cyber-risque porte en lui une dimension systémique : celle de la défaillance simultanée d'une proportion massive d'assurés. La probabilité de tels événements est accrue par l'utilisation d'outils numériques présentant des vulnérabilités identiques par un nombre important d'acteurs : indépendamment de la question des mises à jour, le nombre restreint de systèmes d'exploitation transforme une vulnérabilité utilisée par des hackers en sinistre qui touche une part considérable du portefeuille. De même, l'attaque d'un serveur *cloud*, identifié comme scénario à risque dans le rapport de la Lloyd's, a des conséquences sur un large nombre d'usagers. Dans cette situation, la mutua-

lisation n'opère plus. Quand bien même le coût individuel pour chaque assuré serait faible, la défaillance simultanée met en danger le modèle économique.

Cette modélisation du risque d'accumulation est un véritable enjeu de la constitution d'une cyber-assurance stable et viable. Pour le prendre en compte, la donnée classique (historique de pertes) ne suffit pas, même si elle reste fondamentale. Elle doit s'enrichir d'expertises, provenant des professionnels de la cyber-sécurité, d'une part, – leur appréciation technique du risque est en effet fondamentale –, mais doit probablement puiser également dans d'autres champs disciplinaires, d'autre part. Les phénomènes de contagion – financière, épidémique – sont largement étudiés dans d'autres secteurs. Un enjeu à court terme sera de les adapter au contexte particulier du cyber risque, à sa cinétique et à ses mécanismes particuliers.

Conclusion

La construction d'un écosystème d'assurance cyber viable apparaît donc comme un élément crucial de la protection contre cette menace qui frappe l'ensemble de la société. Face à la cyber-malveillance, il s'agit bien sûr de prévenir, mais aussi de savoir guérir et réparer. Le coût économique de cette protection doit donc être évalué de façon fine, afin de cerner la part qui peut être prise en charge par les assureurs ou la collectivité. Derrière cette évaluation apparaît le double enjeu de la modélisation des risques et de la constitution de bases de données fiables nécessaires à leur calibration. Le comportement des acteurs est un élément essentiel, à la fois dans la prévention ou la réponse donnée aux incidents, et il possède un impact tout à fait considérable sur les analyses quantitatives qui peuvent être menées. Au-delà de la conception de services innovants pour les victimes, déjà à l'œuvre dans le secteur de l'assurance, la construction de modèles adaptés s'affirme comme un enjeu scientifique fort. La résilience de notre société face aux cyber-menaces dépendra notamment de leur robustesse.

Notes

1. Rapport *État de la menace numérique en 2019*, https ://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019.

2. Rapport *Counting the Risk - Decoding Cyber-Exposure*, https ://www.lloyds.com > files > risk-insight > cyence.

BIBLIOGRAPHIE

ABBRING J. H., HECKMAN J. J., CHIAPPORI P. A. et PINQUET J. (2003), « Adverse Selection and Moral Hazard in Insurance: Can Dynamic Data Help to Distinguish? », *Journal of the European Economic Association*, vol. 1, n° 2-3, pp. 512-521.

BÜHLMANN H. et GISLER A. (2006), *A Course in Credibility Theory and its Applications*, Springer Science & Business Media.

CHARPENTIER A. et DENUIT M. (2004), *Mathématiques de l'assurance non-vie*, *Economica.*

CHEN Q. et BRIDGES R. A. (2017), « Automated Behavioral Analysis of Malware: a Case Study of Wannacry Ransomware », in *16th IEEE International Conference on Machine Learning and Applications* (ICMLA), IEEE, pp. 454-460.

DÉNIZ E. G., VÁZQUEZ POLO F. J. et BASTIDA A. H. (2000), « Robust Bayesian Premium Principles in Actuarial Science », *Journal of the Royal Statistical Society: Series D (The Statistician)*, vol. 49, n° 2, pp. 241-252.

ELING M. et LOPERFIDO N. (2017), « Data Breaches: Goodness of Fit, Pricing and Risk Measurement », *Insurance: Mathematics and Economics*, vol. 75, pp. 126-136.

FARKAS S., LOPEZ O. et THOMAS M. (2019), « Cyber Claim Analysis through Generalized Pareto Regression Trees with Applications to Insurance Pricing and Reserving », *Working Paper*, https://hal.archives-ouvertes.fr/hal-02118080/.

FAYI S. Y. A. (2018), « What Petya/NotPetya Ransomware Is and What its Remidiations Are », in *Information Technology-New Generations*, Springer, Cham, pp. 93-100.

FORREST S., HOFMEYR S. et EDWARDS B. (2016), « Hype and Heavy Tails: a Closer Look at Data Breaches », *Journal of Cybersecurity*, vol. 2, n° 1, pp. 3-14.

GRESSIN S. (2017), « The Equifax Data Breach: What to Do », US Federal Trade Commission, 8 septembre.

KESAN J. P., MAJUCA R. P. et YURCIK W. J. (2004), « The Economic Case for Cyberinsurance », University of Illinois, *Law and Economics Working Papers*.

LOW P. (2017), « Insuring Against Cyber-Attacks », *Computer Fraud & Security*, vol. 2017, nº 4, pp. 18-20, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(17)30034-9.

MANSFIELD-DEVINE S. (2015), « The Ashley Madison Affair », *Network Security*, n° 9, pp. 8-16.

NAVETTA D., SEGALIS B., LOCKER E. et HOFFMAN A. (2017), « Wanna Cry Ransomware Attack Summary », Data Protection Report, http://www.dataprotectionreport.com/2017/05/wannacry-ransomware-attack-summary/.

PARK S. C., KIM J. H. et AHN J. Y. (2018), « Does Hunger for Bonuses Drive the Dependence between Claim Frequency and Severity? », *Insurance: Mathematics and Economics*, vol. 83, pp. 32-46.

UMA M. et PADMAVATHI G. (2013), « A Survey on Various Cyber Attacks and their Classification », *IJ Network Security*, vol. 15, n° 5, pp. 390-396.

UNTERSINGER M. (2017), « Le piratage de TV5 Monde vu de l'intérieur », *Le Monde 10 juin 2017,* https://www.lemonde.fr/pixels/article/2017/06/10/le-piratage-de-tv5-monde-vu-de-l-interieur_5142046_4408996.html.