SECTION CONJOINTE DE LA GESTION DU RISQUE

Publié par

GESTION DU RISQUE

JUILLET 2020

Un scénario de pandémie : Le risque systémique ultime?

par Florian Richard

Il y a exactement un an, le bulletin *Gestion du risque* proposait un article de Mario DiCaro, ancien président du Conseil de la Section conjointe de la gestion du risque (SCGR), qui portait plus particulièrement sur la possibilité que **les risques puissent tomber dans l'oubli** en l'absence d'un plan clair sur la façon de gérer les zones de responsabilités croisées en matière de risque au sein d'une organisation. Il avait utilisé une analogie selon laquelle deux joueurs de volleyball performant l'un à côté de l'autre au sein de la même équipe sont responsables de leur propre zone du terrain, jusqu'à ce que le ballon en réception soit sur le point de toucher le sol exactement à la limite de leurs deux zones. En l'absence d'une stratégie claire, le ballon touche inévitablement le sol, ce qui se traduit par un point à l'équipe adverse.

La plupart des types de risques d'assurance semblent s'inscrire dans des catégories de risque manifestement plus vastes – catastrophes naturelles, scénarios de crédit, événements d'origine humaine – parce que, même s'ils sont de nature systémique, ces risques influent sur une gamme principale de produits **ou** sur plusieurs gammes de produits qui sont corrélées dans une certaine mesure.

Toutefois, de quel secteur de responsabilité en matière de risque devrait relever le risque de pandémie, dans la mesure où un scénario peut s'étendre à la plupart des secteurs d'activité existants, que ce soit de façon directe ou indirecte?

Même avant que la COVID-19 ne commence à changer nos vies au début de l'année, le risque de pandémie était déjà à l'avant-plan de la plupart des sociétés d'assurances IARD et d'assurance-vie. Cela s'explique principalement par le fait qu'une poignée d'épidémies locales majeures s'étaient déjà développées dans le monde au cours de la dernière décennie. Chacune de ces épidémies locales nous a appris quelque chose de différent : la possibilité d'annulation d'un événement majeur en raison du virus Zika, la grave contagion et les taux de décès de l'Ebola, la perturbation à court terme des chaînes d'approvisionnement de base pendant l'épidémie de SRAS… La projection de ces types de scénarios à l'échelle mondiale avait déjà l'apparence de ce qui pourrait être considéré comme le **risque systémique ultime**.

Les derniers mois n'ont fait que renforcer cette impression préliminaire. Nous avons découvert que l'impact ne se limite pas seulement aux sinistres, mais vise aussi les primes futures. Même si l'assurance-vie et l'assurance-maladie semblent les gammes de produits les plus touchées, la plupart des nouvelles de l'industrie sont plutôt axées sur l'annulation d'événements, l'interruption éventuelle de l'activité et l'indemnisation des travailleurs. Les gouvernements d'États sont soudainement devenus des acteurs clés dans les discussions sur l'assurance de biens.

À moins d'un scénario de type « fin du monde », existe-t-il un autre exemple de risque avec ce type de portée?

Les sociétés font de leur mieux pour établir un cadre exhaustif de gestion des risques dans lequel les responsabilités en matière de risque sont claires et communiquées à l'échelle de l'organisation. Ainsi, les services de gestion du risque d'entreprise (GRE) peuvent s'assurer que toutes les sources d'exposition susceptibles d'être touchées par ce risque sont déclarées en temps opportun aux fins d'agrégation. La gestion du risque de pandémie exige un effort coordonné pour **toutes** les fonctions de gestion du risque et **toutes** les gammes de produits. En effet, on pourrait soutenir que ce risque exige son propre cadre et sa propre gouvernance au sein d'une organisation.

J'aimerais en savoir davantage sur l'expérience des membres de la SCGR en matière d'évaluation du risque de pandémie, avant et après la COVID-19. Au cours des prochains jours, vous recevrez tous un courriel vous invitant à répondre à un sondage qui portera précisément sur cette question dans plusieurs secteurs d'activité en assurance-vie et en assurances IARD.

Nous avons hâte de recevoir vos commentaires et de partager les résultats des sondages dans le bulletin de décembre. ■

Florian Richard, FCAS, est responsable de la gestion des risques chez AXA XL Reinsurance. Vous pouvez le joindre à *florian.richard@axaxl.com*.

September 15–17, 2020

Online Event

Jointly Sponsored by:

CAS
Expertise. Insight. Solutions.®

American Academy of Actuaries
Objective. Independent. Effective.™

CASUALTY · LOSS · RESERVE · SEMINAR

C · L · R · S

REGISTER TODAY!
casact.org/clrs

SECTION CONJOINTE DE LA GESTION DU RISQUE

Publié par

GESTION DU RISQUE

JUILLET 2020

Cadre de gouvernance des modèles : Les rudiments

par Tricia Matson, Ruth Zea et Amy Alves

Note de la rédaction : Le « Cadre de gouvernance des modèles : Les rudiments », de Tricia Matson, Ruth Zea et Amy Alves constitue un excellent point de départ pour le spécialiste des risques qui établit un nouveau cadre ou qui est sur le point de réévaluer un cadre existant. En plus de traiter de tous les aspects du cycle d'un modèle, le présent article donne un aperçu de la norme ASOP 56, qui entrera en vigueur en octobre 2020 et deviendra la norme de l'industrie à l'avenir.

Nous invitons le lecteur qui souhaite en apprendre davantage à ce sujet à écouter l'enregistrement de la séance sur la gouvernance des modèles animée par Tricia Matson au Symposium sur la gestion du risque d'entreprise de 2020, dans lequel elle approfondit les concepts énoncés dans le présent article et elle les applique ensuite à des études de cas.

Les organisations financières utilisent largement des modèles mathématiques, statistiques et déterministes complexes. Les sociétés d'assurances ont recours à des techniques et des modèles quantitatifs pour diverses raisons : établissement d'une stratégie d'affaires, gestion des risques, calcul du capital réglementaire, surveillance et établissement des limites internes, calcul des expositions, tarification de divers produits, exécution de simulations de crise, etc. L'utilisation de modèles dans le processus décisionnel expose ces institutions à un risque de modélisation indésirable.

À la fin des années 1990, on a accordé plus d'attention aux normes de modélisation dans le secteur des assurances pour tenir compte du rôle de la modélisation des catastrophes dans le cas des ouragans et des tremblements de terre. Depuis, le nombre et l'importance des applications de modélisation dans ce secteur ont considérablement augmenté. À la suite de la dernière crise financière, la réglementation exerce de plus en plus de pression sur la pertinence des modèles des institutions financières. Les organismes de réglementation remettent en question les hypothèses et les limites des modèles, la qualité des données utilisées pour leur étalonnage et la rigueur et l'indépendance du processus de validation des modèles. Ils ont souligné l'importance d'adopter un cadre de gouvernance des modèles d'entreprise pour tenir compte des risques tout au long du cycle de vie d'un modèle.

Les organismes de réglementation s'attendent à ce que la haute direction et les utilisateurs remettent en question la convenance d'un modèle à son utilisation prévue et qu'ils comprennent les limites du modèle qui pourraient influencer sa capacité de respecter l'utilisation prévue. Les limites d'un modèle comprennent, entre autres, les données et les hypothèses. Les hypothèses utilisées dans les modèles devraient être remises en question pour déterminer la pertinence des modèles dans des situations réelles. En particulier, les circonstances dans lesquelles les hypothèses ne seraient plus valables devraient être claires pour les utilisateurs du modèle.

Compte tenu de l'utilisation accrue de la modélisation et de l'importance croissante qui lui est accordée, le Conseil [américain] des normes actuarielles (CNA) a commencé à élaborer une norme de pratique actuarielle (ASOP) axée sur

Le type et le degré du risque de modélisation varient souvent d'un modèle à l'autre et ils peuvent dépendre à la fois du but visé par le modèle et de la nature et de la complexité du modèle.

la modélisation, et quatre exposés-sondages ont été publiés entre 2013 et 2018. En décembre 2019, l'ASOP sur la modélisation a été adoptée par le CNA et elle entrera en vigueur le 1er octobre 2020.[1] L'ASOP 56, *Modeling*, renferme des conseils sur la conception, l'élaboration, la sélection, la modification, l'utilisation, l'examen ou l'évaluation des modèles.

DÉFINITION D'UN MODÈLE

Avant l'adoption de l'ASOP sur la modélisation, l'une des principales sources de conseils sur la gestion du risque de modélisation provenait du Bureau des gouverneurs de la Réserve fédérale dans ses lettres de surveillance et de réglementation sur la gestion du risque de modélisation :

> Le terme « modèle » s'entend d'une méthode, d'une approche ou d'un système quantitatif qui applique des théories, techniques et hypothèses statistiques, économiques, financières ou mathématiques servant à transformer des intrants en estimations quantitatives.[2]

De plus :

> La définition du modèle couvre également les approches quantitatives dont les intrants sont partiellement ou entièrement qualitatifs ou fondés sur le jugement d'experts, à condition que les extrants soient de nature quantitative.

Dans l'ASOP 56, le CNA définit le « modèle » comme suit :

> Représentation simplifiée des relations entre les variables, entités ou événements réels à l'aide de concepts et d'équations statistiques, financiers, économiques, mathématiques, non quantitatifs ou scientifiques. Un modèle se compose de trois éléments : des intrants (renseignements), qui transmettent des hypothèses et des données au modèle, le traitement, qui transforme les intrants en estimations, et des résultats, qui convertissent les estimations en renseignements opérationnels utiles.[3]

La nouvelle norme définit le « risque de modélisation » comme suit :

> Le risque de conséquences défavorables découlant du recours à un modèle qui ne représente pas adéquatement ce qui est modélisé, ou le risque de mauvaise utilisation ou d'interprétation erronée.

OBJET DE LA GOUVERNANCE D'UN MODÈLE

Le risque de modélisation doit être évalué et, s'il est important, il doit être atténué par la gouvernance et les contrôles du modèle. Le type et le degré du risque de modélisation varient souvent d'un modèle à l'autre et ils peuvent dépendre à la fois du but visé par le modèle et de la nature et de la complexité du modèle, y compris ses limites. Un cadre officiel de gouvernance des modèles, qui comprend des politiques et des procédures servant à gérer le risque de modélisation d'entreprise, permet d'appliquer de façon cohérente les stratégies d'atténuation du risque de modélisation et de confirmer que le modèle est bien contrôlé tout au long de son cycle de vie.

Nous avons relevé plusieurs catégories de risque de modélisation :

- **Risque de conception.** Lacunes d'un modèle imputables à une logique ou à une méthodologie défectueuse, ou à un déséquilibre théorique.
- **Risque lié aux données.** Risque attribuable à une qualité ou à une quantité insuffisante de données pertinentes.
- **Risque de mise en œuvre.** Risque découlant de la conversion de modèles en un environnement de production et de l'intégration de modèles à un processus organisationnel, ce qui comprend les inexactitudes numériques, les problèmes technologiques, les bogues de code source, etc.
- **Risque d'étalonnage.** Risque de ne pas adapter correctement le modèle aux situations réelles auxquelles l'entreprise est confrontée.
- **Risque d'utilisation.** Risque d'utilisation incorrecte du modèle, d'interprétation inexacte des résultats du modèle ou de limites imposées par le contexte dans lequel le modèle est utilisé.

ÉLÉMENTS CLÉS ET CYCLE DE VIE D'UN MODÈLE

Dix éléments clés constituent un cadre de gouvernance efficace d'un modèle :

1. **Élaboration.** La gestion du risque de modélisation débute par l'élaboration, lorsque s'amorce le concept d'un nouveau modèle. Les éléments les plus importants du processus sont peut-être à l'œuvre à ce moment, y compris le travail des développeurs qui mettent à profit leur expérience pour définir le modèle.
2. **Documentation.** Une documentation écrite qui décrit chaque étape du processus est essentielle pour cerner rapidement et facilement les composantes du modèle et la capacité d'effectuer un examen de l'efficience et la validation. Elle aide également à atténuer le risque lié aux personnes clés qui est associé aux modèles.
3. **Validation.** Cette étape est considérée comme la phase fondamentale pour mettre les modèles à l'essai et classer leur solidité. La validation consiste à vérifier les méthodes statistiques utilisées, l'information sur les intrants et les extrants, et le rendement. Du point de vue de la gouvernance, les éléments importants à prendre en compte

comprennent l'indépendance des validateurs, la fréquence de la validation, le niveau de la procédure de validation à exécuter compte tenu de l'objet et de la complexité prévus du modèle, et la documentation requise pour appuyer et justifier les procédures de validation exécutées.

4. **Approbation.** Un processus officiel d'approbation des modèles est essentiel pour l'établissement d'un cadre complet de gouvernance des modèles. L'approbation est un élément essentiel pour les institutions financières, elle aide à justifier une bonne gouvernance auprès des organismes de réglementation et elle favorise la responsabilisation individuelle.

5. **Mise en œuvre.** À cette étape, le modèle est mis en production et il est géré par les utilisateurs. Le risque représente la possibilité que certaines composantes de base, comme les renvois aux sources d'origine, les codes d'exécution du modèle et/ou les documents techniques, puissent être perdues. Un cadre central de gouvernance du modèle régissant tout le cycle de vie du modèle est essentiel pour gérer le risque associé aux transferts et à l'atténuation de tout risque lié aux personnes clés.

6. **Modification.** À mesure que les modèles sont personnalisés et modifiés, la documentation incomplète ou partiellement complète devient un scénario courant. La documentation pertinente de tous les éléments du modèle, y compris les spécifications, les limites, les intrants et les extrants, est essentielle pour le suivi continu du rendement du modèle.

7. **Surveillance et retrait du modèle.** Le retrait d'un modèle est souvent sous-évalué ou sous-estimé par rapport aux autres étapes. Toutefois, il est essentiel de vérifier si un modèle fonctionne toujours efficacement ou s'il n'est plus applicable compte tenu de la situation actuelle de l'organisation. Le cadre de gouvernance du modèle devrait comprendre des procédures et un protocole de surveillance continue et, au besoin, de retrait du modèle.

8. **Inventaire des modèles.** Un inventaire des modèles est essentiel pour obtenir une vue d'ensemble des modèles actuellement utilisés, des modèles qui sont retirés ou inutilisés, mais qui peuvent être utilisés, des usages du modèle, du niveau de complexité du modèle et d'autres considérations. Les modèles peuvent être simples ou complexes et ils peuvent varier selon le rôle qu'ils jouent au sein d'une organisation. L'inventaire des modèles devrait fournir une vue globale, en saisissant d'un seul point de vue tout ce qui a trait aux modèles. En outre, la classification des modèles peut permettre d'en améliorer l'organisation. Par exemple, le risque lié à un modèle peut être classé en fonction de sa complexité et de son importance relative, de manière à ce que l'inventaire favorise le suivi de tous les objets liés, y compris les usages, les fins, les propriétés, les changements, la documentation, les codes et les données, ainsi que la détermination de chaque étape du cycle de vie du modèle, c'est-à-dire tous les éléments qui contribuent à l'évaluation du risque de modélisation. Un cadre efficace de gouvernance des modèles nécessite souvent l'utilisation d'un inventaire pour s'assurer que tous les modèles soient identifiés, suivis et soumis à des validations continues.

Il est essentiel de vérifier si un modèle fonctionne toujours efficacement ou s'il n'est plus applicable compte tenu de la situation actuelle de l'organisation.

9. **Partage de l'information.** À mesure que la complexité des processus augmente, la communication devient un facteur essentiel pour les parties visées, surtout lorsqu'il existe une relation de dépendance entre les étapes.

10. **Rôles et responsabilités.** Un cadre de gouvernance doit comprendre une description des rôles et des responsabilités, permettant ainsi un meilleur partage de l'information pour appuyer et régir l'ensemble du processus lié au cycle de vie du modèle.

INTERVENANTS

Le cadre de gouvernance des modèles comprend souvent, à titre de pratique exemplaire, une fonction distincte de la gestion du risque de modélisation chargée d'établir et de tenir à jour le cadre, les politiques et les contrôles de gouvernance des modèles. Ce cadre devrait définir clairement les rôles et les responsabilités des divers intervenants, y compris à l'intérieur et à l'extérieur de la fonction de la gestion du risque de modélisation. Les principaux intervenants comprennent habituellement les personnes suivantes :

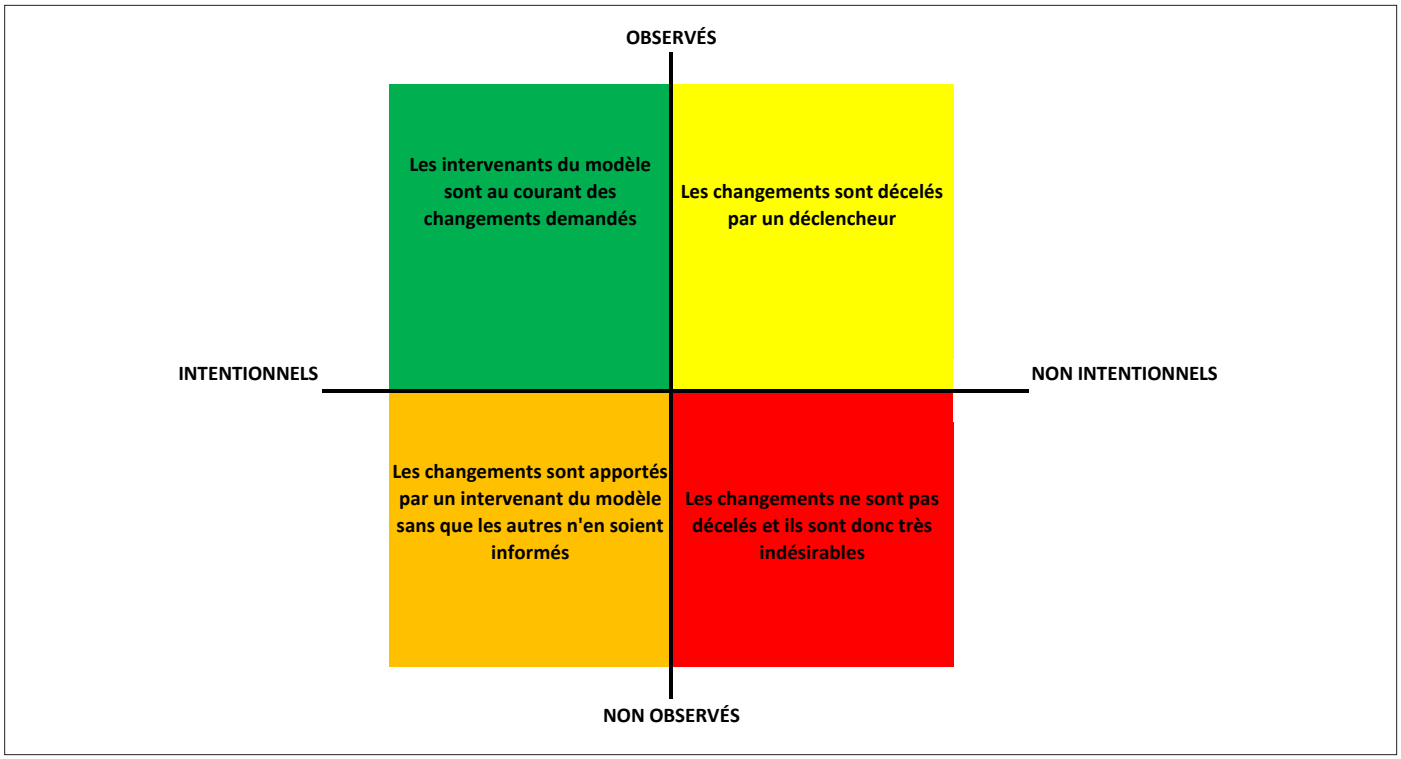
- **Responsable du modèle.** Personne qui demande et, en fin de compte, « possède » le modèle. Le responsable du modèle établit les exigences opérationnelles du modèle, il est chargé des essais d'acceptation par l'utilisateur final et il veille à la bonne mise en œuvre du modèle pour les autres utilisateurs, y compris aux plans de la formation et de la communication, et pour d'autres tâches.

- **Développeur du modèle.** Personne chargée de l'élaboration, du codage, de la mise à l'essai, de l'examen et de la documentation du modèle, conformément aux exigences réglementaires et opérationnelles.

- **Validateur du modèle.** Personne indépendante du processus d'élaboration du modèle, chargée de la validation ou de la mise à l'essai du modèle.

- **Approbateur du modèle.** Personne chargée d'approuver le modèle et la documentation connexe avant la mise en œuvre. Dans certains cas, il s'agit d'un comité plutôt que d'une personne.

Figure 1
Quatre types de changement dans les modèle



- **Utilisateurs du modèle.** Personnes ou équipes qui utilisent le modèle ou les résultats du modèle au quotidien. Habituellement, l'entreprise qui demande l'élaboration du modèle, c'est-à-dire le responsable du modèle, est le principal utilisateur du modèle.
- **Exécutant du modèle.** Les modèles peuvent être mis en œuvre comme des processus autonomes ou intégrés à l'infrastructure de TI d'une organisation. L'exécutant du modèle est chargé de mettre en production le modèle approuvé aux fins d'utilisation.

LIGNES DE DÉFENSE RÉGISSANT LE RISQUE DE MODÉLISATION

Le risque de modélisation peut se concrétiser à n'importe quelle étape du cycle de vie d'un modèle. Par conséquent, les intervenants du modèle font partie du principe des trois lignes de défense :

- **Première ligne.** Représentée par les activités opérationnelles, la première ligne porte sur l'élaboration du modèle, les activités et la disponibilité.
- **Deuxième ligne.** La fonction de gestion des risques est chargée d'élaborer des procédures de gestion du risque de modélisation et des exigences de validation. La surveillance du rendement du modèle relève habituellement de la deuxième ligne, qui doit vérifier la cohérence, la validité et l'efficacité du modèle.
- **Troisième ligne.** Pour brosser le tableau complet de la gouvernance, la troisième ligne de défense traite avec les auditeurs, elle évalue les activités en vue d'une analyse efficace et efficiente du risque de modélisation et elle signale les lacunes et les améliorations apportées aux processus.

LES CHANGEMENTS APPORTÉS AU MODÈLE ET LE RISQUE

Les modèles peuvent faire l'objet de changements mineurs ou majeurs à n'importe quelle étape de leur cycle de vie, particulièrement dans le cas des modèles de tableurs autonomes, qui sont très sensibles au changement.

En général, il existe quatre types de changement, qui peuvent être représentés de façon graphique sur les axes des changements observés-non observés et intentionnels-non intentionnels (figure 1).

Tous les changements peuvent être classés en fonction de leur incidence, par exemple, faible, moyenne, élevée et urgente.

Selon le type et l'ampleur du changement, le processus de gestion du modèle doit prévoir des mesures pertinentes pour gérer et atténuer le risque associé aux changements apportés au modèle.

MOT DE LA FIN

La gestion du nombre croissant de modèles, souvent de plus en plus complexes et sophistiqués, peut être difficile et elle entraîne souvent un niveau accru de risque de modélisation assumé par

une organisation. Un cadre de gouvernance de modèle bien conçu et correctement mis en œuvre est essentiel et de première importance pour atténuer ce risque.

Lorsqu'on établit le cadre de gouvernance des modèles qui convient à une organisation donnée, il faut tenir compte de plusieurs facteurs.

- **Cadre personnalisé.** La gouvernance du modèle doit être adaptée aux besoins de l'organisation. Il ne s'agit pas d'un cadre « universel ». La gouvernance du modèle devrait dépasser une simple procédure, en tenant compte des besoins, des priorités, des complexités et du contexte de l'organisation.
- **Proportionnalité.** Les coûts et les avantages doivent être pris en compte aux fins de l'atténuation du risque de modélisation. L'évaluation de l'importance relative par rapport au risque et à la valeur économique devrait orienter les décisions sur l'affectation des travaux et des ressources.
- **Uniformité du processus.** De façon générale, les cadres de gouvernance des modèles devraient être uniformes pour tous les modèles. Toutefois, dans certains cas, les modèles dont l'importance relative ou le potentiel de risque sont faibles peuvent être assujettis à des exigences moins rigoureuses.
- **Cadre pragmatique.** Le cadre de gouvernance du modèle vise à gérer le risque de modélisation. Il doit être aussi clair et simple que possible, sans ajouter de risques supplémentaires.

Comme nous l'avons mentionné, l'utilisation de modèles dans le processus décisionnel expose les organisations à un risque de modélisation indésirable. Toutefois, un bon cadre de gouvernance des modèles peut réduire sensiblement ce risque, ce qui permet aux entreprises de se concentrer sur ce que leur révèlent les modèles. ■

Tricia Matson, FSA, MAAA, est associée chez Risk & Regulatory Consulting, LLC. Vous pouvez la joindre à *tricia.matson@riskreg.com*.

Ruth Zea, FCAS, MAAA, peut être jointe à *ruthzea.451@hotmail.com*.

Amy Alves, CPA, MCM, est gestionnaire principale chez Risk & Regulatory Consulting, LLC. Vous pouvez la joindre à *amy.alves@riskreg.com*.

NOTES

1 Pour la version finale approuvée de la norme, voir le Conseil des normes actuarielles, *Norme de pratique actuarielle nº 56*, décembre 2019, *http://www.actuarialstandardsboard.org/wp-content/uploads/2020/01/asop056_195.pdf* (consulté le 26 juin 2020).

2 SR 11-7 : Guidance on Model Risk Management, Conseil des gouverneurs du système de la Réserve fédérale, 4 avril 2011, *https://www.federalreserve.gov/supervisionreg/srletters/sr1107.htm* (consulté le 1er juillet 2020).

3 Conseil des normes actuarielles, Norme de pratique actuarielle no 56, décembre 2019, *http://www.actuarialstandardsboard.org/wp-content/uploads/2020/01/asop056_195.pdf* (consulté le 26 juin 2020).

SECTION CONJOINTE DE LA GESTION DU RISQUE

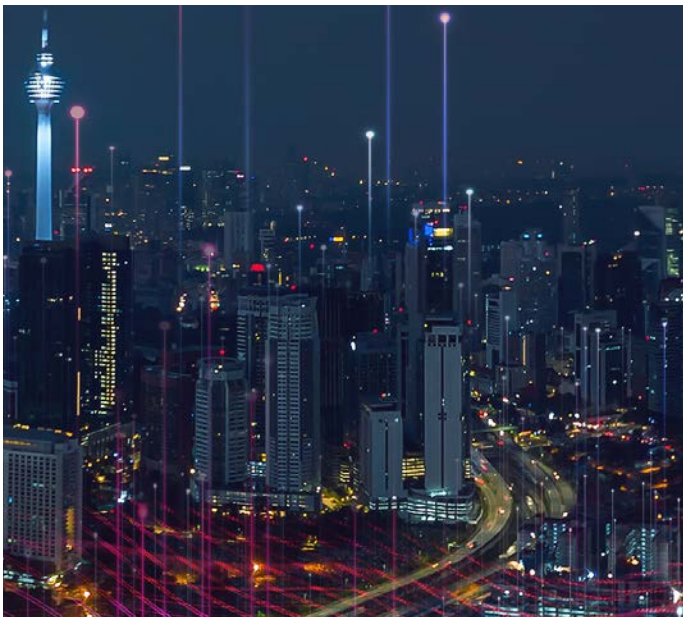
Publié par

GESTION DU RISQUE

JUILLET 2020

Cybersécurité : Composer avec la question de l'exclusion relative à la guerre

par Chris Harner, Chris Beck et Blake Fleisher



Note de la rédaction : Dans le marché sans cesse croissant de la cyberassurance, le libellé des polices est souvent au cœur des discussions des professionnels de l'assurance. Le présent article constitue un suivi des discussions du groupe d'experts sur le cyberrisque qui ont eu lieu à l'assemblée annuelle et exposition de la Society of Actuaries en 2019.

Après avoir décrit les principales affaires judiciaires connues de l'industrie, les auteurs décrivent les problèmes associés à la définition et à l'application de cette clause.

Comme le nombre et l'intensité des cyberattaques augmentent à l'échelle mondiale, le marché de la cyberassurance est en croissance. Selon une analyse, la valeur du marché mondial de la cyberassurance s'élevait à 4,3 milliards de dollars en 2018 et elle devrait atteindre près de 16,7 milliards en 2024.[1] Environ 50 % des entreprises américaines ont contracté une assurance contre le cyberrisque.

De plus en plus, les assureurs considèrent le cyberespace comme un risque et ils peinent à le modéliser, à souscrire et à tarifer des polices et à déterminer le risque d'accumulation. Outre les défis classiques que posent l'obtention de riches ensembles de données et la compréhension des corrélations, les assureurs doivent tenir compte de l'incertitude entourant le caractère exécutoire du libellé des polices, plus précisément l'exclusion relative à la guerre.

De façon générale, les milieux juridique et militaire ne s'entendent pas sur la définition de la guerre, et encore moins de la guerre dans le cyberespace. Il s'agit d'une question pertinente – en fait, c'est le thème central de l'affaire Mondelez v. Zurich en cours devant la Cour du Circuit du Comté de Cook en Illinois.[2] La réponse à cette question est loin d'être claire. Les clauses d'exclusion relative à la guerre ont longtemps été présentées comme des questions difficiles et elles sont remplies d'exceptions dans l'espace physique conventionnel. Les caractéristiques exclusives du cyberconflit, comme l'attribution, le refus plausible, le fardeau de la preuve, la complexité et l'interdépendance, ajoutent à l'ambiguïté de ce qui est considéré comme un acte de guerre dans le cyberespace. Bien que ces questions ne soient pas réglées, nous visons à les cerner pour que des décisions pertinentes sur la modélisation puissent être prises.

Bon nombre des affaires judiciaires portant sur la question de l'exclusion relative à la guerre comportent des conclusions simples, ce qui complique la recherche de précédents clairs. En fait, certains arguments présentés dans les diverses affaires semblent se contredire, de sorte qu'il est difficile de déterminer si l'assureur ou le titulaire est responsable. Un examen exhaustif de la jurisprudence dépasse la portée du présent document. Pour démontrer cette ambiguïté, nous étudierons plutôt certaines affaires historiques dans l'espace physique qui ont traité de l'exclusion relative à la guerre.

AFFAIRES DANS LESQUELLES LES TRIBUNAUX ONT STATUÉ EN FAVEUR DU TITULAIRE

Airlift International Inc. v. United States

En juin 1967, pendant la guerre du Vietnam, un avion Constellation de type L-109H d'Airlift International était en plan de vol entre les Philippines et le Vietnam, en vertu d'un contrat du Military Airlift Command des États-Unis. Quelques

minutes avant l'atterrissage, il a été percuté par un appareil RF-4C de l'Aviation américaine. Le pilote et le navigateur du RF-4C se sont éjectés avec succès et ils ont survécu, mais tous les occupants de l'avion d'Airlift International sont décédés et l'avion a été détruit.

Les demandes de règlement en assurance ont été rejetées par l'assureur en raison de la clause d'exclusion relative à la guerre. En fin de compte, les tribunaux ont statué que la collision était attribuable à un risque aérien qui pourrait exister en temps de paix. Ils ont donc conclu que la demande de règlement était admissible à l'assurance.[3]

Pan American World Airways, Inc. v. Aetna Casualty and Surety Co.

En 1970, le Front Populaire pour la Libération de la Palestine a effectué plusieurs détournements d'avions commerciaux, connus sous le nom de détournements du terrain d'aviation de Dawson. Le vol 93 de la Pan Am, de Bruxelles à New York, n'est jamais arrivé au terrain de Dawson. L'appareil a plutôt atterri au Caire après un bref arrêt à Beyrouth pour faire le plein. À l'atterrissage en Égypte, le 6 septembre 1970, l'avion a explosé presque immédiatement après le débarquement des passagers et de l'équipage.[4]

Les dommages ont été estimés à 24,3 millions de dollars. Les assureurs ont fait valoir que le sinistre était visé par les clauses d'exclusion relative à la guerre des polices tous risques — plus précisément que le sinistre avait été directement causé par [traduction libre] « la capture, la saisie […] ou l'action d'une armée […] ou un pouvoir usurpé », en vertu de « la guerre […] la guerre civile, la révolution, la rébellion, l'insurrection ou les opérations de guerre » ou par « des émeutes [ou] des mouvements civils ». Toutefois, le gouvernement des États-Unis, qui offrait une protection d'assurance contre le risque de guerre en sus de celle offerte par des souscripteurs privés, a soutenu que le rejet du sinistre était attribuable à un acte de baraterie de la part du transporteur.[5] Les tribunaux ont statué que les assureurs tous risques étaient responsables de la totalité du sinistre. Cette décision s'explique en partie par le fait qu'en 1969, les souscripteurs d'assurance aviation offraient une clause d'exclusion couvrant expressément les détournements, et Aetna aurait pu utiliser cette clause lorsqu'elle a souscrit la protection. En ne le faisant pas, [traduction libre] « elle a agi à ses propres risques ».[6]

Holiday Inns, Inc. v. Aetna Insurance Co.

Pendant la guerre civile du Liban, l'hôtel Holiday Inn de Beyrouth a été lourdement endommagé lors de la Bataille des hôtels. Lorsque Holiday Inns Inc. a demandé une protection en vertu de sa police d'assurance tous risques, la société d'assurances Aetna a refusé cette demande en invoquant la clause d'exclusion relative à la guerre. Toutefois, les tribunaux ont tranché en faveur de Holiday Inns Inc. Le juge a écrit : [traduction libre] « L'hôtel Holiday Inn a été endommagé par une série de « mouvements populaires » de plus en plus violents. Le pays a frôlé l'anarchie. Mais le gouvernement constitutionnel a toujours existé, et l'intention requise de le renverser n'a pas été prouvée, sauf pour ce qui est d'autres interprétations et il n'y a pas eu de « guerre » au Liban entre États souverains ou quasi souverains. »[7] Étant donné que Holiday Inns Inc. a payé une surprime pour les « mouvements populaires », elle avait droit à la protection prévue par la police.

AFFAIRES DANS LESQUELLES LES TRIBUNAUX ONT STATUÉ EN FAVEUR DE L'ASSUREUR

TRT/FTC Communications Inc. v. Insurance Company of State of Pennsylvania

En décembre 1989, le Panama a déclaré la guerre aux États-Unis. Panama City était dans un état de désordre civil, et TRT, une entreprise de télécommunications, y exploitait une installation de vente. Pendant ce temps, des hommes armés portant des vêtements civils se sont introduits dans les locaux de TRT à Panama City, et ils ont volé des marchandises et de l'équipement.

L'assureur a prétendu que la protection ne s'appliquait pas en raison de la clause d'exclusion relative à la guerre. Les tribunaux ont statué que [traduction libre] « peu importe que les hommes fassent partie des forces panaméennes ou d'un groupe de pilleurs, il existe de nombreux éléments de preuve à l'appui de la conclusion selon laquelle leurs actions contre TRT ont été facilitées par les hostilités militaires entre le Panama et les États-Unis ».[8] La position de l'assureur a donc été confirmée.

New York Life Ins. Co. v. Bennion

Le 7 décembre 1941, le capitaine Bennion, commandant de l'USS West Virginia (BB-48), a perdu la vie lorsque son navire a été coulé à Pearl Harbor pendant l'attaque japonaise. Son épouse, Louise Bennion, a intenté une poursuite contre la New York Life Insurance Company pour le double de l'indemnité de 10 000 $ qui lui était due advenant le décès « accidentel » de son mari. La société a payé le principal prévu en vertu de la police de 10 000 $. Toutefois, la police la dispensait de l'obligation de double indemnité. Cette clause a soulevé la question de savoir si le pays était en guerre lorsque Pearl Harbor a été attaqué ou lorsque le Congrès a déclaré la guerre le lendemain.

La New York Life Insurance Company n'a eu aucune difficulté à prouver que tous les intervenants ont considéré l'attaque comme un acte de guerre et, en rendant une décision favorable à la société d'assurances, le tribunal a déclaré qu'il est bien connu que l'attaque de Pearl Harbor « a lancé » la guerre.[9]

EXCLUSIONS RELATIVES À LA GUERRE ET CYBERATTAQUES

Aussi difficile soit-il de déterminer s'il existe des motifs d'exclusion relative à la guerre dans l'espace physique, il est encore plus difficile de le déterminer dans le cyberespace. Cela s'explique en partie par le fait que les cyberattaques représentent une forme relativement nouvelle de conflit, mais aussi par certaines caractéristiques uniques du cyberespace. Certains principes fondamentaux de l'exclusion relative à la guerre dans l'espace physique peuvent encore s'appliquer, notamment le précédent d'ambiguïté du libellé de la police. Comme nous l'avons vu dans l'affaire Pan Am v. Aetna, si le libellé de la police est ambigu, ou si l'assureur avait pu utiliser un libellé qui l'exclurait clairement et qu'il avait choisi de ne pas l'utiliser, le tribunal pourrait trouver une protection là où il le souhaite. Néanmoins, même avec ce fondement dans l'espace physique, il subsiste de nombreuses inconnues.

Lorsqu'il s'agit de déterminer si une cyberattaque constitue un acte de guerre, l'attaque contre Sony vient à l'esprit.

Sony Pictures

En 2014, des pirates nord-coréens ont prétendument commis une infraction à l'endroit de Sony Pictures en représailles à son film satirique *The Interview*. Bien que l'administration du président Obama ait attribué l'attaque à la Corée du Nord, elle s'est délibérément abstenue de qualifier d'« acte de guerre » l'attaque menée par un acteur étatique. Probablement consciente des clauses d'exclusion relative à la guerre dans les polices d'assurance, l'administration a plutôt qualifié l'attaque de « cybervandalisme ».[10]

Sony était protégée par l'assureur sans que la clause d'exclusion relative à la guerre pose problème malgré le fait que la Corée du Nord est un acteur étatique.[11] Cependant, les victimes de cyberattaques ne sont pas toutes aussi chanceuses.

NotPetya

Le 27 juin 2017, la Russie a prétendument propagé le ver NotPetya au moyen d'un logiciel fiscal ukrainien pour cibler l'infrastructure ukrainienne.[12] Vous trouverez des renseignements plus détaillés sur cette attaque dans le livre blanc de Milliman intitulé *The Law of Unintended Consequences: When Companies Are Collateral Damage in a Cyberattack*.[13]

Le ver NotPetya s'est propagé rapidement et a touché des entreprises partout dans le monde, dont l'expéditeur mondial Maersk, la société pharmaceutique Merck et la société de grignotines Mondelez International. Ces entreprises n'étaient pas les cibles, mais plutôt les dommages collatéraux d'une cyberattaque à grande échelle d'acteurs étatiques.

Mondelez International, en particulier, s'est fait voler de nombreux justificatifs d'identité, et 1 700 de ses serveurs et 24 000 de ses ordinateurs portables ont été détruits. La multinationale spécialisée dans les grignotines était propriétaire d'une police d'assurance de biens tous risques qui, selon elle, couvrait à la fois les pertes physiques directes et les dépenses indirectes encourues pendant une panne informatique.[14] Mondelez estime les dégâts à plus de 100 millions de dollars. Toutefois, l'assureur, Zurich American Insurance, a rejeté la demande en invoquant la clause d'exclusion relative à la guerre :

> [traduction libre] « B. La présente police exclut les pertes ou les dommages causés directement ou indirectement ou découlant de l'une ou l'autre des causes ou événements suivants, qu'ils soient assurés ou non en vertu de la présente police, et qui contribuent simultanément ou dans toute autre séquence à la perte :
>
> …
>
> 2) (a) une action hostile ou belliqueuse en temps de paix ou de guerre, y compris une action visant à entraver, à combattre ou à se défendre contre une attaque réelle, imminente ou attendue par :
>
> (i) un pouvoir gouvernemental ou souverain (de droit ou de fait);
>
> (ii) les forces militaires, navales ou aériennes;
>
> (iii) le mandataire ou l'autorité d'une partie mentionnée en (i) ou (ii) ci dessus.[15]

Mondelez a soutenu que sa protection d'assurance ne résulte pas d'une cause ou d'un événement précisé dans la clause d'exclusion relative à la guerre et que Zurich a refusé à tort cette protection. Selon la plainte, la haute direction de Zurich a reconnu que le refus de la protection était abusif et inapproprié, et la société a promis à Mondelez qu'elle annulerait son refus de protection

et elle a finalement accepté d'effectuer un paiement partiel de dix millions de dollars qui était inconditionnel et non assujetti à une disposition de « récupération ».[16] Cependant, malgré l'annulation du refus de protection par Zurich, Mondelez n'a jamais reçu les fonds et a décidé de poursuivre Zurich.

L'issue de cette affaire aura probablement des répercussions très importantes sur la cyberassurance. Si le tribunal statue en faveur de Mondelez, les assureurs pourraient devoir repenser s'ils souhaitent continuer à souscrire une branche d'assurance dans laquelle les tribunaux n'appliqueront pas l'exclusion relative à la guerre, même si les acteurs étatiques jouissent de la plus grande capacité de déclencher des sinistres. Ils devront aussi revoir leur libellé de souscription, car l'ambiguïté de la clause d'exclusion relative à la guerre amène souvent les tribunaux à se prononcer en faveur des souscripteurs. À l'inverse, si le tribunal statue en faveur de Zurich, les sociétés devront alors se demander s'il est logique de contracter une assurance qui ne paie pas lorsqu'un acteur étatique leur cause un préjudice important.

Outre les répercussions de la validité de l'exclusion relative à la guerre, les tribunaux devront répondre à l'une des questions les plus fondamentales, c'est-à-dire déterminer ce qui constitue un acte de guerre dans le cyberespace. Selon la façon dont on répond à cette question, il se peut que les assureurs soient incapables d'invoquer la clause d'exclusion relative à la guerre dans le but de refuser la protection. Compte tenu de l'historique des affaires judiciaires concernant la guerre « traditionnelle », il semble que les demandes de règlement doivent être tranchées au cas par cas. Puisque les acteurs étatiques sont si profondément enracinés dans la cyberguerre et que les sociétés peuvent être attaquées involontairement n'importe où dans le monde, les définitions générales des cyberactes de guerre pourraient mener à l'inutilité de la cyberassurance. Par ailleurs, certaines définitions pourraient rendre la clause d'exclusion relative à la guerre essentiellement inutile, auquel cas les paiements d'assurance pourraient dépasser la prime prévue, ce qui pourrait entraîner la non-rentabilité de l'assurance de dommages liée à la cybersécurité.

CARACTÉRISTIQUES EXCLUSIVES DU CYBERESPACE

Certaines caractéristiques exclusives du cyberespace compliquent particulièrement la question de l'exclusion relative à la guerre. Dans la présente section, nous examinons trois de ces caractéristiques : la possibilité d'un déni plausible, le fardeau de la preuve, et la complexité et l'interdépendance.

Déni plausible

Parmi les nouveautés de la cybercriminalité, mentionnons qu'il est relativement difficile d'attribuer une attaque à certains intervenants parce que les pirates, en particulier les acteurs étatiques, sont capables de couvrir leurs traces. Ainsi, les pirates jouissent d'un déni plausible, qui est souvent une qualité très recherchée dans les conflits géopolitiques. D'une certaine façon, un déni plausible permet aux acteurs étatiques de poursuivre certaines actions qui ne sont peut-être pas conformes à l'ensemble actuel des lois et normes internationales. Cela dit, bien qu'il soit difficile de déterminer l'identité d'un pirate dans le cyberespace, la tâche n'est pas impossible. Les États-nations et les entreprises de cybersécurité recourent fréquemment à des techniques judiciaires numériques pour identifier l'auteur de cyberattaques à un certain niveau de probabilité.

Fardeau de la preuve

Même s'il est possible d'identifier un pirate avec un certain degré de confiance, le fardeau de la preuve incombe toujours aux sociétés d'assurances. Par exemple, les agences de renseignements sur les acteurs étatiques ne dévoilent jamais les fins détails des méthodes qu'elles utilisent pour attribuer l'attaque à un acteur particulier, en partie pour ne pas rendre publics leurs propres outils et capacités, mais également pour ne pas divulguer des renseignements très secrets ou compromettre les opérations en cours. Il se pourrait aussi que dans certains cas, un acteur étatique ne souhaite pas attribuer publiquement l'attaque à un pays particulier si la divulgation ne correspond pas à ses intérêts nationaux du moment. En outre, le fait de s'en remettre aux garanties données par des sociétés ou des gouvernements tiers soulève des questions : quelles déclarations d'attribution de sociétés et États-nations sont valables pour une demande de règlement d'assurance? En outre, même si l'attaque est attribuée à un acteur particulier, quel est le degré de vraisemblance nécessaire pour l'attribution? Quel genre et quelle quantité d'information sont nécessaires? Toutes ces questions doivent probablement être réglées sous une forme ou sous une autre lorsqu'il s'agit de déterminer si une société d'assurances peut invoquer sa clause d'exclusion relative à la guerre.

Complexité et interdépendance

Comme on l'a vu dans l'affaire NotPetya, en raison de la nature interconnectée du cyberespace, il est difficile de déterminer si une entreprise était la cible. D'une certaine façon, toutes les sociétés pourraient constituer une proie en cas d'attaque de la part d'un acteur étatique même si elles n'exercent pas leur activité près d'une zone de guerre. Non seulement est-il plus difficile pour les sociétés de se protéger, mais il est encore plus difficile pour les actuaires de modéliser le risque. En particulier, il existe beaucoup d'incertitude dans le système juridique, compte tenu de ce qui semble être l'absence d'un précédent global unique. En outre, une société en région éloignée, où le crime est très peu répandu, pourrait devenir un dommage collatéral d'une cyberattaque perpétrée par un acteur étatique. Ce type d'action est très difficile à prévoir, mais les actuaires et les souscripteurs doivent en tenir compte dans leur évaluation du risque.

CONCLUSION

L'incertitude qui plane sur ces préoccupations juridiques et réglementaires complique la compréhension et la modélisation du cyberrisque. Plus particulièrement, les enjeux soulevés dans le présent article mettent en lumière des questions de protection fondamentales que devront intégrer les modèles de tarification futurs. Selon toute vraisemblance, la jurisprudence évoluera lentement en ce qui concerne la façon dont les tribunaux peuvent percevoir les cyberattaques et leurs conséquences. Compte tenu de l'ambiguïté des définitions juridiques, il est important de bien réfléchir aux conséquences directes et indirectes d'une cyberattaque déclarée comme un acte de guerre. ■

Chris Harner, FRM, est directeur général du groupe Cyber Risk Solutions chez Milliman. Vous pouvez le joindre à *chris.harner@milliman.com*.

Chris Beck est conseiller auprès de la direction en gestion des risques au sein du groupe Cyber Risk Solutions chez Milliman. Vous pouvez le joindre à *chris.beck@milliman.com*.

Blake Fleisher est analyste principal du cyberrisque au sein du groupe Cyber Risk Solutions chez Milliman. Vous pouvez le joindre à *blake.fleisher@milliman.com*.

NOTES

1 Dwyer, K. Cyber Insurance Capacity Could Quadruple in Six Years; Don't Let Your Coverage lag. Dans *Risk & Insurance*. 6 mars 2020. https://riskandinsurance.com/commercial-cyber-insurance-could-quadruple-in-six-years-dont-let-your-coverage-lag/ (en anglais seulement) (consulté le 24 mai 2020).

2 Mondelez International Inc. v. Zurich American Insurance Company (Circuit Court, Cook County, Illinois. 2016). https://www.scribd.com/document/397265756/Mondelez-Zurich (consulté le 24 mai 2020).

3 Airlift International, Inc. v. United States, 335 F. Supp. 442 (S.D. Fla. 1971). https://law.justia.com/cases/federal/district-courts/FSupp/335/442/1737917/ (consulté le 24 mai 2020).

4 Avis de décès de B. Marquard : À 84 ans, John Ferruggio, héros du détournement du vol de la Pan Am en 1970. *Boston Globe*, le 22 juin 2010. http://archive.boston.com/bostonglobe/obituaries/articles/2010/06/22/john_ferruggio_of_milton_hero_of_1970_pan_am_hijacking_dies_at_84/ (consulté le 24 mai 2020).

5 Dans ce contexte, le transporteur fait référence au transporteur aérien Pan American World Airways Inc.

6 Evans, Alona E. 1975. Pan American World Airways, Inc. c. The Aetna Casualty and Surety Co. Et Al. *The American Journal of International Law* 69, vol 2, pp. 415 431. doi:10.2307/2200277 (consulté le 28 avril 2020).

7 Lewin, T. Beirut Insurance Ruling Favors Holiday Inns. *New York Times*, 21 septembre 1983, https://www.nytimes.com/1983/09/21/business/beirut-insurance-ruling-favors-holiday-inns.html (consulté le 24 mai 2020).

8 Caban, E.E. 2003. War-risk, Hijacking and Terrorism Exclusions in Aviation Insurance: Carrier Liability in the Wake of September 11, 2001. *Journal of Air Law and Commerce* 68, vol 2, no 8. https://scholar.smu.edu/jalc/vol68/iss2/8 (consulté le 24 mai 2020).

9 Borchard, E. 1947. When Did the War Begin? *Columbia Law Review*.https://digitalcommons.law.yale.edu/fss_papers/3413/ (consulté le 24 mai 2020).

10 Satariano, A., et N. Perlroth. Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong. *New York Times*, 15 avril 2019, https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html (consulté le 5 juin 2020).

11 Rand, J.M. A. A Tale of Two Carriers: Disparate Views of War/Terrorism Exclusion. *Cyberinsurance Law Blog*, 28 mars 2019, https://www.databreachninja.com/a-tale-of-two-carriers-disparate-views-of-war-terrorism-exclusion/ (consulté le 24 mai 2020).

12 Greenberg, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History. *par voie câblée*, le 22 août 2018, https://www.wired#.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/?verso=true (consulté le 24 mai 2020).

13 Harner, C., C. Beck et B. Fleisher. *The Law of Unintended Consequences: When Companies Are Collateral Damage in a Cyberattack*. Livre blanc Milliman. Le 9 mars 2020. https://us.milliman.com/fr/insight/the-law-of-unintended-consequences-when-companies-are-collateral-damage-in-a-cyberattack (consulté le 24 mai 2020).

14 Corcoran, B. What Mondelez v. Zurich May Reveal About Cyber Insurance in the Age of Digital Conflict. *Lawfare*, 8 mars 2019 https://www.lawfareblog.com/what-mondelez-v-zurich-may-reveal-about-cyber-insurance-age-digital-conflict (en anglais seulement) (consulté le 24 mai 2020).

15 Mondelez v. Zurich, précité, note 2.

16 Ibid.