Mémoire présenté devant Sorbonne Université et l'ISUP pour l'obtention du Master de Sciences Mention Actuariat et l'admission à l'Institut des Actuaires

Par : Mathieu VILTIE
Titre : Tarification des polices cyber par approche proie-prédateur

Confidentialité : ☐ Non ☑ Oui (Durée : ☐ 1 an ☑ 2 ans)

Les signataires s'engagent à respecter la confidentialité ci-dessus

Membres présents du jury de l'Institut des Actuaires :

Entreprise :
Nom : SeaBird Conseil
Signature :

Membres présents du Jury du Master Actuariat de l'ISUP :

Directeur de Mémoire en entreprise :
Nom : Baptiste DIELTIENS
Signature :

Autorisation de publication et de mise en ligne sur un site de diffusion de documents actuariels (après expiration de l'éventuel délai de confidentialité)

Secrétariat :

Bibliothèque :

Signature du responsable entreprise

Signature du candidat

Résumé

Mots clés : risque cyber, proie-prédateur, lissage Whittaker-Henderson, tarification, indice de risque

Le risque cyber impose de nouveaux défis aux assureurs. Parmi ces derniers, les questions de tarification sont une préoccupation majeure car les conséquences financières ne sont pas anodines. Aujourd'hui, la problématique d'assurabilité de ce risque est encore très présente chez les assureurs au vu du manque de connaissance et de gestion du risque cyber.

Cette étude consiste à élaborer une méthode de tarification basée sur la création d'un indice de risque qui sera exclusivement construit à l'aide de la sinistralité observée d'un portefeuille d'assurés.

Ce modèle est fondé sur l'approche proie-prédateur (Lotka-Volterra), dont l'implémentation nécessite le calibrage de plusieurs paramètres. Une fois ce dernier implémenté, une méthode de tarification basique sera élaborée permettant la détermination des primes par police cyber.

Dès lors que les primes auront été déterminées, une analyse de sensibilité sur les différentes hypothèses sera effectuée. En effet, un certain nombre d'hypothèses ont été prises par manque de données. C'est pourquoi, nous rediscuterons de ces dernières dans une dernière partie.

Abstract

Keywords : cyber risk, prey-predator, Whittaker-Henderson smoothing, pricing, risk index

Cyber risk imposes new challenges on insurers. Among these, pricing issues are a major concern because the financial consequences are not trivial. Today, the problem of insurability of this risk is still very present among insurers due to the lack of knowledge and management of cyber risk.

This study consists of developing a pricing method based on the creation of a risk index that will be constructed exclusively using the observed loss experience of a portfolio of policyholders.

This model is based on the prey-predator approach (Lotka-Volterra), the implementation of which requires the calibration of several parameters. Once the latter is implemented, a basic pricing method will be developed to determine the premia per cyber policy.

Once the premia have been determined, a sensitivity analysis of the different assumptions will be performed. Indeed, a number of assumptions have been made due to the lack of data. For this reason, we will discuss these assumptions again in a final section.

Note de Synthèse

Cadre de l'étude

Selon le site gouvernemental français, le risque cyber est défini comme l'atteinte à des systèmes informatiques réalisée dans un but malveillant. Quatre types d'attaques aux conséquences diverses sont différenciés, affectant directement ou indirectement les particuliers, les administrations ainsi que les entreprises :

- Cybercriminalité ;
- Atteinte à l'image ;
- Espionnage ;
- Sabotage.

La gestion du risque cyber est un enjeu majeur aujourd'hui de part une mauvaise connaissance de ce dernier mais également par une croissance des assureurs à vouloir proposer des polices cyber. Ainsi, de plus en plus d'acteurs seront amenés à travailler sur ces sujets sans pour autant connaître de méthode ou de base de données « reconnue » permettant la modélisation de ces risques.

Le but de cette étude consiste à proposer une approche tarifaire permettant de déterminer une prime à une police d'assurance cyber par la construction d'un indice de risque basé exclusivement sur la sinistralité d'un portefeuille d'assuré. De ce fait, ce papier s'éloignera des méthodes usuelles de tarification (de type coût-fréquence).

Dans un premier temps, nous étudierons théoriquement le modèle de Lotka-Volterra. Puis, nous nous intéresserons aux conséquences et résultats sur la structure du portefeuille de la compagnie étudiée.

Modèle de Lotka-Volterra

L'indice de risque que nous souhaitons créer doit varier de la façon suivante : lorsque l'indice de risque cyber augmente, le nombre d'attaques réussies doit également augmenter. En effet, cet indice est semblable à un indice de menace ou encore de « vulnérabilité » que les entreprises ont face aux évènements cyber. A l'inverse, plus l'indice de risque diminue, moins les entreprises auront tendances à ce que les attaques réussissent.

Cependant, il faudra prendre en compte un temps de décalage entre la dynamique de cet indice et la dynamique des sinistres. Si l'indice de risque augmente à un instant t, le nombre d'attaques ne va pas augmenter à l'instant t mais augmentera à un instant $t + \delta$ ($\delta > 0$). Afin de pouvoir modéliser tous ces éléments, nous nous sommes donc

orientés vers le modèle de Lotka-Volterra où il est possible d'établir un lien direct entre cet indice et le niveau de sinistralité. Le modèle que nous utilisons est une variante du modèle proie-prédateur. En effet, lorsque le modèle a été crée, le phénomène de base ne tenait pas compte d'une possibilité d'extinction de l'une des populations. Les paramètres utilisés dans la modélisation des deux dynamiques ont tendance à se compenser. C'est pourquoi, nous aurons toujours des courbes qui peuvent varier au cours du temps mais qui n'auront pas de tendance sur l'ensemble de la fenêtre d'observation. En effet, considérons une entreprise qui connaît son niveau de menace face au risque cyber. Elle prendra sûrement plusieurs mesures de sécurité sur du court terme faisant baisser à un instant donné les attaques. Cependant, cette dernière pourra également décider d'agir sur le long terme ce qui diminuera pérennement la sinistralité cyber. C'est pourquoi une variante a été proposée et s'exprime de la façon suivante : pour tout temps t,

$$\begin{cases} \frac{dy_1(t)}{dt} = y_1(t)\big(a - by_2(t)\big) + et; \\ \frac{dy_2(t)}{dt} = y_2(t)\big(-c + dy_1(t)\big) - et. \end{cases} \qquad \text{avec } y_1(t_0) = y_1(0),\ y_2(t_0) = y_2(0).$$

Table 1 – Description des variables du modèle

Variable	Description
t	Mois
$y_1(t)$	Indice de risque cyber - proies
$y_2(t)$	Nombre d'attaques réussies / Nombre de sinistres - prédateurs
$\frac{dy_1(t)}{dt}$	Variation de l'indice de risque cyber au cours du temps
$\frac{dy_2(t)}{dt}$	Variation du nombre de sinistres au cours du temps
$a > 0$	Taux de croissance de l'indice de risque
$b > 0$	Facteur de déclin de l'indice de risque
$c > 0$	Facteur de déclin du nombre de sinistres
$d > 0$	Taux de croissance du nombre de sinistres
e	Facteur de développement ou d'extinction de l'une des populations

Comme il n'est pas possible de réaliser ce modèle sur de la sinistralité brute, nous avons préalablement lissé cette dernière à l'aide du lissage de Whittaker-Henderson. Cette méthode permet de concilier deux objectifs contradictoires :

- Critère de fidélité : les $\hat{q}_x$ (estimation de la sinistralité) doivent être proches des q_x (sinistralité brute) car ce sont des estimateurs non paramétriques (aucune hypothèse n'a été effectuée) ;
- Critère de régularité : nous avons un *a priori* sur la courbe qui doit être lisse. Cependant, la courbe des sinistres brutes ne l'est pas.

L'objectif de la modélisation sera de trouver le meilleur compromis entre le critère de fidélité et le critère de régularité. Après lissage, le modèle de Lotka-Volterra a été calibré sur cette dernière et est représenté de la façon suivante :

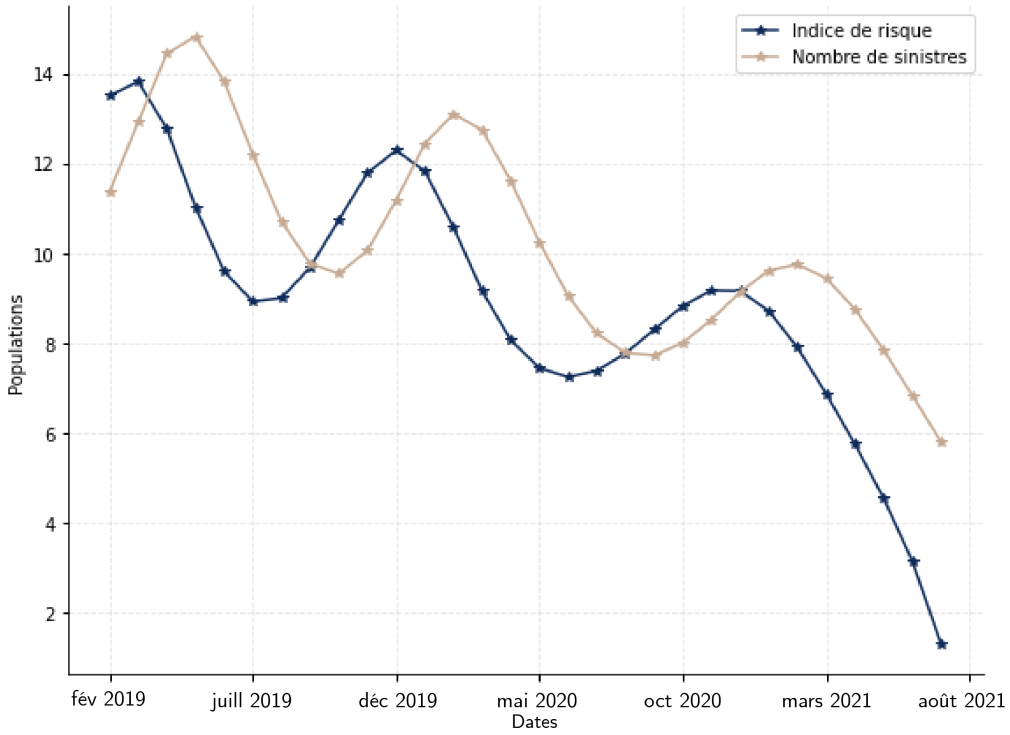

FIGURE 1 – Modèle de Lotka-Volterra

Tarification

La méthode de tarification que nous proposons est décomposée en deux étapes :

- Étape 1 : normaliser l'indice de risque afin qu'il appartienne à l'intervalle $[0, 1]$;
- Étape 2 : application d'un taux de prélèvement sur le chiffre d'affaires de l'entreprise.

Une fois que ces deux étapes ont été réalisées, il est alors possible de déterminer la prime pure. En notant :

- ent_j l'entreprise j ;
- $C(ent_j)$ le chiffre d'affaires de l'entreprise j ;
- i le taux annuel prélevé sur le chiffre d'affaire constant ;
- $\phi(x)$ l'indice de risque cyber de l'entreprise j.

Alors, la prime est déterminée par :

$$\pi(ent_j) = i \times C(ent_j) \times \phi(x).$$

La seule variable inconnue dans la détermination de la prime est le taux annuel à prélever sur le chiffre d'affaires. Afin de déterminer ce dernier, nous avons calibré nos S/P sur l'étude LUCY de l'AMRAE pour l'année 2019. L'analyse portera donc sur l'année 2020 ainsi que 2021.

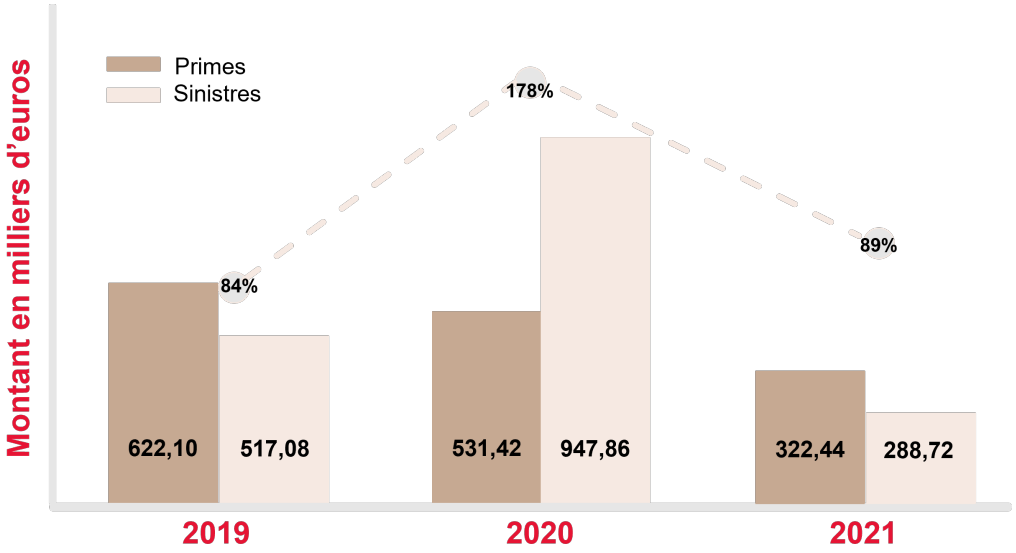

FIGURE 2 – Représentation des S/P globaux avec un taux de 1,30%

Ce graphique est à mettre en lumière avec l'étude de l'AMRAE (rapport LUCY). Ces données permettent de mieux comprendre la saturation que connaît le marché de l'assurance cyber. Les assureurs bénéficient de réduction du volume des primes en 2020 avec un volume de sinistre qui croît, ceci impactant leur solvabilité. Ce phénomène est principalement dû à la crise sanitaire en 2020. En effet, lorsque nous regardons le début d'année 2021, nous observons que le volume global des primes est supérieur à celui des indemnisations. De ce fait, le ratio S/P est passé de 178% en 2020 à 89% en 2021 soit une diminution de 89 points de pourcentage.

A l'aide du tableau ci-dessous, lorsque nous regardons selon la maille métier, le montant des S/P est très disparate d'une entité à l'autre. Les métiers ayant le plus fort S/P entre 2019 et 2021 sont les collectivités ainsi que les associations. Les collectivités rassemblent les communes, les établissements publiques ou encore les établissements scolaires. Ce sont des organisations qui semblent avoir des infrastructures les moins adoptées aux dangers cyber.

TABLE 2 – Représentation des S/P selon le type de métiers

Type de métiers	2019	2020	2021
PROFESSIONNEL	127%	198%	40%
ENTREPRISE	78%	53%	112%
COLLECTIVITE	381%	618%	176%
AGRICOLE	27%	155%	58%
CONSTRUCTION	147%	109%	132%
ASSOCIATION	132%	255%	1135%

Synthesis note

Scope of the study

According to the French government website, cyber risk is defined as the attack on computer systems carried out with malicious intent. Four types of attacks with various consequences are differentiated, directly or indirectly affecting individuals, administrations as well as companies :

- Cybercrime ;
- Damage to image ;
- Espionage ;
- Sabotage.

The management of cyber risk is a major issue today due to a lack of knowledge of the latter but also due to the growth of insurers wanting to offer cyber policies. Thus, more and more actors will be required to work on these subjects without knowing a method or a « recognized » data base allowing the modeling of these risks.

The purpose of this study is to propose a pricing approach to determine a premium for a cyber insurance policy by constructing a risk index based exclusively on the loss experience of an insured portfolio. Therefore, this paper will move away from from the usual pricing methods (cost-frequency approach).

First, we will study the theory of the Lotka-Volterra model. Then, we will look at the consequences and results on the structure of the portfolio of the studied company.

Lotka-Volterra model

The risk index we want to create should vary in the following way : when the cyber risk index increases, the number of successful attacks should also increase. In fact, this index is similar to a threat index or « vulnerability » index that companies have when faced with cyber events. Conversely, as the risk index decreases the less likely companies are to have successful attacks.

However, a time lag between the dynamics of this index and the dynamics of claims must be taken into account. If the risk index increases at time t, the number of attacks will not increase at time t but will increase at time $t + \delta$ ($\delta > 0$). In order to model all these elements, we have turned to the Lotka-Volterra model where it is possible to establish a direct link between this index and the level of claims. The model we use is a variant of the prey-predator model. Indeed, when the model was created, the basic phenomenon did not

take into account the possibility of extinction of one of the populations. The parameters used in the modeling of the two dynamics tend to compensate each other. This is why we will always have curves that can vary over time but that will not have a trend over the entire observation window. In fact, let's consider a company that knows its threat level in the face of cyber risk. It will surely take several security measures in the short term to reduce attacks at a given moment. However, the company may also decide to act in the long term, which will reduce the cyber loss rate on a permanent basis. This is why a variant has been proposed and is expressed as follows : for any time t,

$$\begin{cases} \frac{dy_1(t)}{dt} = y_1(t)\big(a - by_2(t)\big) + et; \\ \frac{dy_2(t)}{dt} = y_2(t)\big(-c + dy_1(t)\big) - et. \end{cases} \quad \text{with } y_1(t_0) = y_1(0),\ y_2(t_0) = y_2(0).$$

Table 3 – Model variables description

Variable	Description
t	Month
$y_1(t)$	Cyber risk index - preys
$y_2(t)$	Number of successful attacks / Number of claims - predators
$\frac{dy_1(t)}{dt}$	Variation of the cyber risk index over time
$\frac{dy_2(t)}{dt}$	Variation of successful attacks over time
$a > 0$	Growth rate of the risk index
$b > 0$	Risk index decline factor
$c > 0$	Decline factor in the number of claims
$d > 0$	Growth rate of the number of claims
e	Factor of development or extinction of one of the populations

As it is not possible to run this model on raw claims, we have first smoothed the latter using a Whittaker-Henderson smoothing. This method allows us to reconcile two contradictory objectives :

- Fidelity criterion : the $\hat{q}_x$ (loss estimate) must be close to the q_x (gross loss) because they are non-parametric estimators (no hypothesis has been made) ;
- Regularity criterion : we assume the curve must be smooth. However, the gross claims curve is not.

The objective of the modeling will be to find the best compromise between the fidelity and regularity criteria. After smoothing, the Lotka-Volterra model has been calibrated on the latter and is represented as follows :

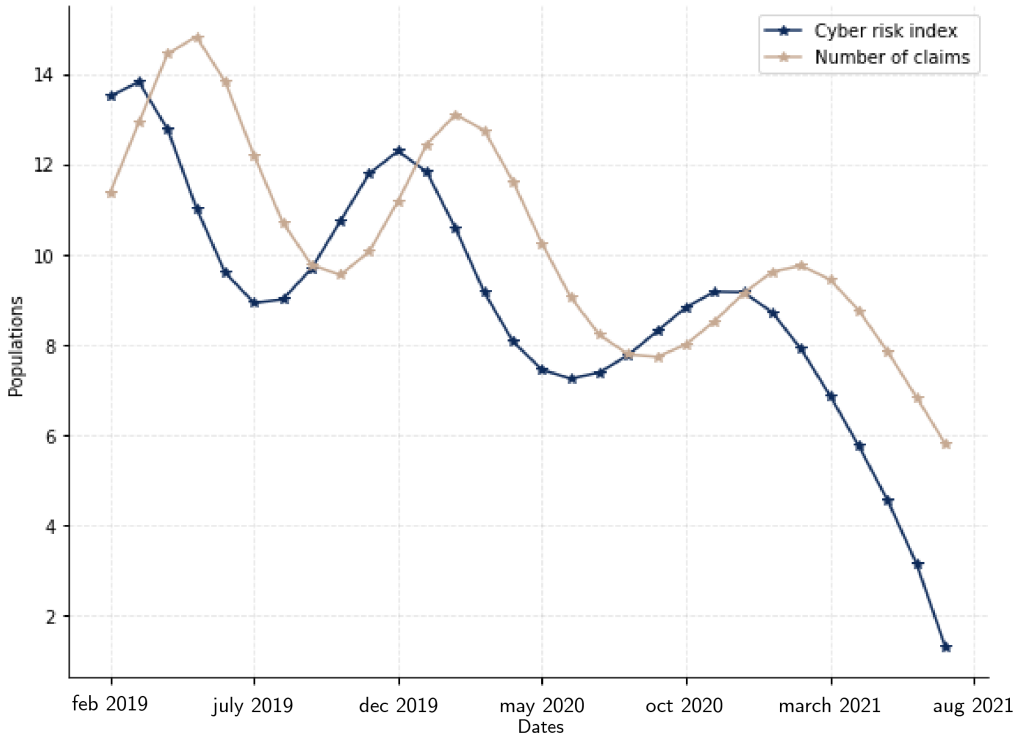

FIGURE 3 – Lotka-Volterra model

Pricing

Our proposed pricing method is broken down into two steps :

- Step 1 : normalize the risk index so that it belongs to the interval $[0, 1]$;
- Step 2 : application of a levy rate on the company's turnover.

Once these two steps have been completed, it is then possible to determine the pure premium. Noting :

- ent_j the compagny j ;
- $C(ent_j)$ the company's turnover j ;
- i the annual rate levied on the turnover constant ;
- $\phi(x)$ the cyber risk index of the company j.

Then the premium is determined by :

$$\pi(ent_j) = i \times C(ent_j) \times \phi(x).$$

The only unknown variable in the determination of the premium is the annual rate to be deducted on the turnover. In order to determine this, we calibrated our loss ratio on the LUCY study for the year 2019. The analysis will therefore cover the year 2020 as well as 2021.

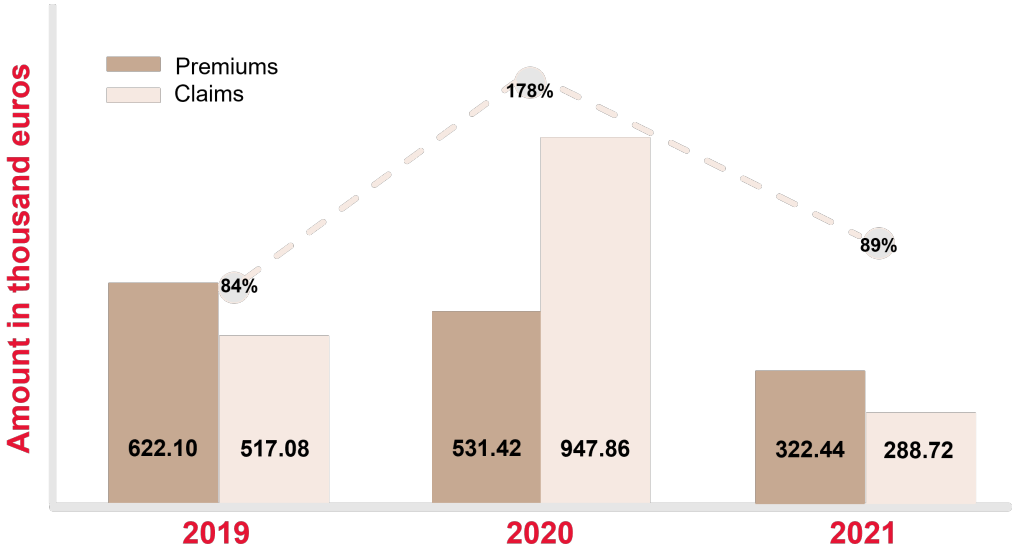

FIGURE 4 – Representation of the global loss ratio with a rate of 1.30%

This graph should be seen in conjunction with the AMRAE study (LUCY report). These data allow us to better understand the saturation of the cyber insurance market. Insurers have benefited from a reduction in premium volume in 2020 with a growing claims volume, which impacts their solvency. This phenomenon is mainly due to the health crisis in 2020. Indeed, when we look at the beginning of 2021, we observe that the overall volume of premia is higher than the volume of claims. As a result, the S/P ratio went from 178% in 2020 to 89% in 2021, a decrease of 89 percentage points.

Using the table below, when we look at the business line, the amount of loss ratio is very disparate from one entity to another. The trades with the highest loss ratio between 2019 and 2021 are communities and associations. The local authorities include municipalities, public institutions and public institutions or schools. These are organizations that seem to have the least adapted infrastructures to cyber dangers.

TABLE 4 – Loss ratio representation by trade type

Type of professions	2019	2020	2021
PROFESSIONAL	127%	198%	40%
COMPANY	78%	53%	112%
COMMUNITY	381%	618%	176%
AGRICULTURAL	27%	155%	58%
CONSTRUCTION	147%	109%	132%
ASSOCIATION	132%	255%	1135%

Remerciements

Tout d'abord, je souhaiterais remercier toutes les personnes ayant contribué à l'élaboration de cette étude.

Plus particulièrement, merci à toute l'équipe de SeaBird Conseil de m'avoir fait confiance lors de mon stage de Master 1 ainsi que lors de mon alternance.

Merci à Baptiste DIELTIENS, mon tuteur ainsi que mon manager qui a su se rendre disponible, à l'écoute et toujours bienveillant en me faisant partager ses conseils et son expertise.

Enfin, je souhaiterai également remercier Olivier LOPEZ pour la qualité de son enseignement durant le cours de cyber assurance et qui m'a accompagné durant la rédaction de ce mémoire.

Table des matières

Introduction

L'usage d'outils numériques s'est considérablement développé ces dernières années et s'est accéléré avec la crise sanitaire. Cette croissance est la conséquence d'un usage massif du télétravail, de l'école en ligne, ou encore des commandes par internet qui ont explosé en raison des fermetures des commerces non essentiels. Contrairement à l'image que l'on peut avoir sur les cybercriminels, ce sont des personnes qui s'organisent de façon extrêmement structurée en formant des équipes sur le *darknet* et qui ont pour but de maximiser leur profit.

Prenons un exemple historique dans le monde cyber : l'incident *WannaCry*. Le 12 mai 2017, un écran inhabituel apparaît sur les postes de travail de plusieurs entreprises. Les machines ont été infectées par *WannaCry*, un rançongiciel. L'accès aux informations contenues dans le serveur infecté est bloqué et une rançon est demandée par les cybercriminels aux victimes.

Ce type d'attaque est classique. Mais, ce qui l'est moins est l'ampleur de cette dernière. *WannaCry* se répandit par internet en une semaine et toucha entre 200 000 et 300 000 victimes à travers 150 pays (selon Avast [4]). Les personnes qui ont été prises pour cible sont des particuliers, des entreprises de toutes tailles, des services de santé, des agences gouvernementales ainsi que des universités. Les dommages ont été estimés à plusieurs milliards de dollars. L'exemple en est avec *National Health Service (NHS)* au Royaume-Uni qui, selon Acronis [1] a perdu 92 millions de livres sterling suite à cet incident. Pour autant, ce ne seraient pas les coûts liés à la rançon qui auraient été dévastateurs pour les victimes mais plutôt les nombreuses pertes induites telles que les pertes d'exploitation.

Contre la montée de cette insécurité numérique, plusieurs solutions de cyber assurance se développent fortement ces dernières années. La principale solution consiste à fournir une aide contre la perte financière. Mais plusieurs autres garanties moins usuelles sont proposées et couplées à des offres de prévention et d'assistance en cas de sinistre. Ces offres sont particulièrement recherchées par les petites et moyennes entreprises n'ayant pas une compétence interne suffisamment riche pour faire face en cas de crise. Ces garanties ont pour but de faciliter l'assistance afin d'augmenter la réactivité permettant d'éviter une aggravation des dommages.

L'incident *WannaCry* a été l'un des éléments déclencheurs dans la prise de conscience du danger des cyber incidents et notamment leur caractère massif. Il faut toutefois noter que tous les évènements cyber ne sont pas forcement massifs et ne touchent pas forcément beaucoup d'acteurs de manière sévère. L'évènement *WannaCry* a été beaucoup médiatisé notamment par le fait qu'il ait touché beaucoup de personnes en très peu de temps.

Ce mémoire propose d'élaborer une méthode de tarification des polices cyber. Pour ce faire, notre analyse portera précisément sur la construction d'un indice de risque permettant de

quantifier le niveau de menace d'une entreprise à un instant donnée. Bien que certaines hypothèses devront être prises par manque de données, nous verrons que les résultats peuvent être comparés à ceux obtenus par des instances officielles (comme l'AMRAE).

Dans une première partie, nous commencerons par définir ce qu'est le risque cyber. Après un bref rappel historique des évènements cyber qui ont eu lieu dans un passé récent, nous présenterons un état des lieux du marché français de l'assurance cyber. Aussi, nous discuterons de la législation en vigueur en France qui a drastiquement évolué au cours des dernières années. Enfin, le dernier point consistera à présenter les études académiques actuelles qui permettent de mieux cerner les enjeux de la cyber assurance.

Dans une seconde partie, nous proposerons un modèle de construction d'indice de risque que nous appliquerons sur une base de données publique sur l'assurance violations de données. Une première discussion concernera la description des données utilisées. Puis, nous présenterons l'intérêt d'une modélisation proie-prédateur ainsi qu'une analyse détaillée des principaux résultats. Quant au dernier point, il consistera à présenter les limites de la modélisation actuelle sur la base de données publique.

Dans une dernière partie, nous appliquerons sur une base de données réelle issu d'un portefeuille français le modèle de Lotka-Volterra. Après un bref descriptif sur les variables présentes dans cette dernière, une analyse sur le nombre d'attaques sera menée conduisant à la création de l'indice de risque. Ainsi, une prime pourra alors être déterminée pour chaque entreprise présente dans le portefeuille. Le niveau des primes obtenues ainsi que le S/P seront remis en question à l'aide d'une étude de sensibilité. Enfin, nous évoquerons les limites rencontrées durant ces travaux.

Chapitre 1

Risque cyber : contexte et enjeux

Ce chapitre a pour objectif d'apporter au lecteur une compréhension globale de ce qu'englobe le risque cyber. Pour ce faire, nous avons réalisé un état des lieux des connaissances que les assureurs possèdent sur ces évènements.

Dans la *première partie*, une définition globale de ce qu'est le risque cyber sera proposée ainsi que les types d'attaques associés.

Dans une *deuxième partie*, un bref rappel historique d'attaque cyber sera présenté.

Puis, dans une *troisième partie*, l'état des lieux du marché de l'assurance cyber sera présenté à l'aide d'une étude publiée par l'AMRAE.

Quant au côté législatif, il sera abordé dans une *quatrième partie*. Cette dernière permettra d'une part de comprendre la gestion du risque actuel mais également de mieux appréhender les questions que les acteurs du marché se posent sur ce type de risque.

Enfin, la *dernière partie*, consistera à présenter les grandes études académiques qui ont permis de mieux cerner les enjeux de la cyber assurance.

1.1 Définition du risque cyber

Dans cette partie, à l'aide du site gouvernemental français, une proposition de ce qu'est le risque cyber ainsi que les différentes attaques qui peuvent être réalisées sera effectuée.

Le risque cyber est défini comme l'atteinte à des systèmes informatiques réalisée dans un but malveillant. Quatre types d'attaques aux conséquences diverses sont différenciés, affectant directement ou indirectement les particuliers, les administrations ainsi que les entreprises.

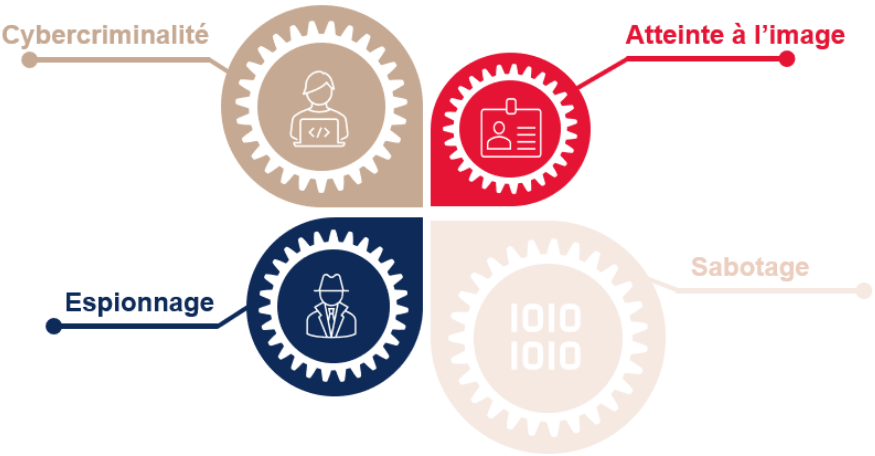

FIGURE 1.1 – Types de cyber-attaques

1.1.1 Cybercriminalité

La cybercriminalité englobe les attaques visant à obtenir des informations personnelles qui seront par la suite exploitées ou revendues. Les victimes de ces attaques sont à la fois les particuliers mais également les entreprises ainsi que les administrations. Les informations bancaires et les identifiants des commerces en ligne sont les principales données ciblées par les cybercriminels.

Deux sortes d'attaques ont été différenciées :

- Attaque par hameçonnage ou *phishing* ;
- Attaque par rançongiciel ou *ransomware*.

L'attaque par hameçonnage ou *phishing* est une méthode très répandue sur internet. Les cybercriminels usurpent l'identité des personnes afin d'obtenir des renseignements personnels ou encore des identifiants bancaires qui permettront d'être utilisés ultérieurement. L'usurpation se fait par le biais de personnes physiques ou morales de confiance. Les *hackers* diffusent un message ou un mail frauduleux pouvant contenir une pièce jointe piégée. Ce dernier invite l'utilisateur à entrer ses informations personnelles, notamment ses coordonnées bancaires sur des sites fictifs vers lesquels ils sont redirigés. Ce type d'attaque ne cible pas une personne en particulier mais plutôt un grand nombre de contacts. En effet, plus le nombre de personnes contactées est grand, plus les chances que l'un d'entre eux ouvre la pièce jointe et/ou entre ses données personnelles sont importantes.

L'attaque par rançongiciel ou *ransomware* est de plus en plus répandue. Les cybercriminels cryptent les données puis demandent aux propriétaires de ces dernières d'envoyer de l'argent en échange d'une clé qui permettra (« théoriquement ») de les décrypter. Pour ce faire, les pirates diffuseront un mail ou un message contenant des liens ou pièces jointes piégées. Par exemple, la victime peut recevoir un mail lui indiquant de payer rapidement une facture qui ne l'a pas été. Dès lors que l'utilisateur cliquera sur le lien ou les pièces jointes, un logiciel se téléchargera directement sur son poste de travail et commencera à crypter ses données personnelles. Les données ciblées sont de toutes sortes : bureautique, vidéos, musiques ou encore photos.

1.1.2 Atteinte à l'image

L'atteinte à l'image consiste à déstabiliser des personnes morales comme des entreprises ainsi que des administrations qui peuvent par la suite être relayées par les réseaux sociaux. Cette méthode a pour objectif de ternir l'image de la victime par divers propos politiques ou encore religieux diffusés sur internet.

Deux sortes d'attaques ont été différenciées :

- Attaque par déni de service (*distributed denial of service attack* ou *ddos*) ;
- Attaque par défiguration (*defacement*).

L'attaque par déni de service (*ddos*) est une méthode consistant à ternir l'image de l'utilisateur. Pour ce faire, les cybercriminels rendront les systèmes d'information en ligne inaccessibles et propageront des revendications politiques, religieuses ou procéderont à des extorsions de fonds. Afin de rendre les sites inaccessibles, ils auront préalablement exploité une vulnérabilité et les ressources du système d'information (disque dur, bande de réseau, ...) de la victime jusqu'à son épuisement.

L'attaque par défiguration (*defacement*) a pour objectif d'altérer l'intégrité de l'entreprise en modifiant l'apparence et le contenu de leur site. Pour ce faire, les cybercriminels exploitent des vulnérabilités du site qui sont connues mais non corrigées. Les *hackers* réalisent ces attaques à des fins politiques, religieuses, mais également pour freiner la concurrence.

1.1.3 Espionnage

L'espionnage consiste à attaquer discrètement des entreprises et des administrations à des fins économiques ou scientifiques. Les cybercriminels sont organisés en groupe ce qui aggrave les conséquences des attaques. L'espionnage peut être perçu par la victime tardivement : il faut parfois plusieurs années à une organisation afin de s'apercevoir qu'elle est espionnée. L'attaque par espionnage a également pour objectif de maintenir discrètement et pérennement l'accès aux cybercriminels afin de capter l'information stratégique en temps voulu.

Deux sortes d'attaques ont été différenciées :

- Attaque par point d'eau (*watering hole*) ;
- Attaque par hameçonnage ciblé (*spearphishing*).

L'attaque par point d'eau (*watering hole*) est une méthode consistant à piéger un site

internet en infectant les équipements des personnes visitant ce dernier. L'objectif des cybercriminels est de récupérer illégalement les données des visiteurs en exploitant les vulnérabilités des sites en ligne grâce au dépôt d'un virus de type *malware*. Ce virus s'installera sur l'ordinateur de la victime et permettra un accès à ce dernier pour le cybercriminel.

L'attaque par hameçonnage ciblé (*spearphishing*) consiste à usurper l'identité d'une personne morale ou physique afin d'infiltrer le système d'information d'une organisation. Dans un premier temps, la victime est invitée à ouvrir une pièce jointe ou un lien. Dès lors, l'ordinateur sera contaminé. Grâce à cela, le cybercriminel pourra prendre le contrôle de ce dernier et pénétrer par la suite le système d'information de l'organisation représentant la véritable cible. Le cybercriminel pourra également demander d'obtenir certains droits (comme les droits d'administrateur) afin de s'implanter sur les autres ordinateurs et serveurs de l'organisation lui permettant de voler un maximum de données.

1.1.4 Sabotage

Le sabotage consiste à attaquer un système informatique en le rendant inopérant en intégralité ou partiellement. L'attaque par sabotage s'apparentera à une panne organisée en frappant des systèmes informatiques. Ces attaques peuvent être assez coûteuses à dédommager et peuvent également être médiatisées. Il existe une multitude de types d'attaque par sabotage car les organisations ne sont, dans la plupart du temps, pas préparées à y faire face. Ces attaques ont pour objectif de nuire à l'organisme victime. Cela aura des conséquences économiques mais également organisationnelles.

La définition du risque cyber ainsi que ses quatre composantes a été proposée par le site gouvernemental français. Cependant, il n'existe pas de définition commune et acceptée de tous par les acteurs de l'assurance. Prenons pour exemple l'étude sur les risques cyber présentée par l'APREF (Association des Professionnels de la Réassurance En France)[3]. Cette dernière définie le risque cyber non pas comme le site gouvernemental français mais plutôt comme « toutes atteintes à :

- Des systèmes électroniques et/ou informatiques [de production, d'exploitation, de gestion d'informations et de télécommunication] sous le contrôle de l'entité ou de ses prestataires et/ou ;
- Des données informatisées (personnelles, confidentielles ou d'exploitation) appartenant à ou sous le contrôle de l'entité, qu'elles soient transférées ou stockées chez elle ou chez ses prestataires.

Consécutives à :

- Un acte malveillant ou de terrorisme ;
- Une erreur humaine, une panne ou des problèmes techniques ;
- Un évènement naturel ou accidentel.

Ayant pour conséquences :

- Des dommages corporels, matériels, et/ou immatériels (frais ou pertes financières), subis par l'entité et/ou ses employés ;
- Une mobilisation de ressources internes ou externes ;
- Des dommages corporels, matériels, et/ou immatériels, frais ou pertes financières causés par l'entité à des tiers (y compris chaînes logistiques / sous-traitants) ;

- Une atteinte à la marque et/ou à la réputation de l'entité. »

Rappelons que les définitions ci-dessus ont été proposées par le gouvernement français. En effet, d'un acteur à un autre, les définitions peuvent donc varier drastiquement, d'où la nécessité de bien comprendre et cerner le périmètre d'étude englobant cette notion de risque cyber.

1.2 Rappel historique d'attaque cyber

Avec le large panel d'évènements cyber pouvant survenir, il semble pertinent de montrer la place du risque cyber parmi les autres risques rencontrés en assurance. La FFA (Fédération Française de l'Assurance) publie une quatrième édition du baromètre des risques élaboré par la Commission Analyse des Risques de la Fédération. Dans cet article [5] et pour la quatrième année consécutive, le risque de cyber-attaques demeure le risque principal qui pèserait sur les sociétés d'assurance et de réassurance. La seconde place est occupée par les risques liés à un environnement économique dégradé. Quant à la troisième place, elle est occupée par le risque épidémique. Afin de mieux comprendre les craintes liées au risque, nous proposons maintenant au lecteur un bref historique d'évènements cyber. Ci-dessous, une frise chronologique relatant divers évènements cyber entre 2017 et 2022 est présentée.

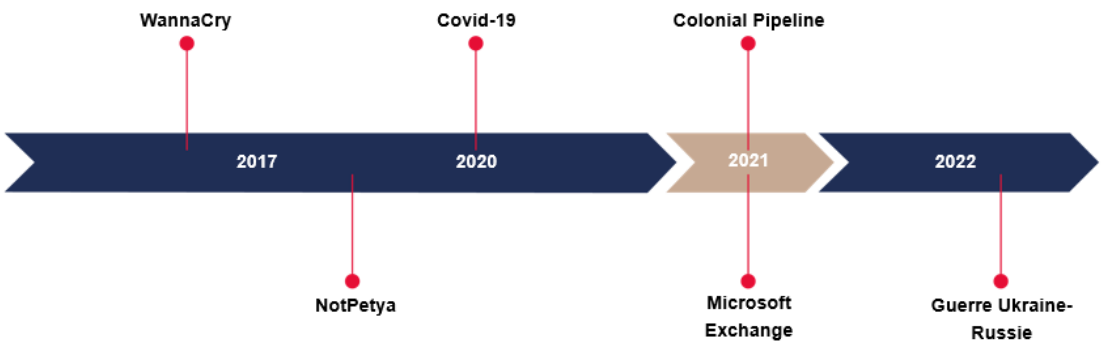

FIGURE 1.2 – Bref historique des cyber-attaques à travers le temps

Détaillons quelques évènements de la frise :

- **NotPetya :** En juin 2017, un logiciel malveillant détruisant les données de type effaceur (*wiper*) apparaît sur les ordinateurs. NotPetya exploite une faille informatique pour toute version de Windows non mise à jour. L'attaque se propage de la façon suivante : une entreprise reçoit un fichier .exe qui infecte l'ordinateur. Une fois ce dernier infecté, il se développe à l'aide du réseau interne. Plusieurs grands groupes ont été touchés et répertorient des pertes d'environ 300 millions d'euros. Prenons l'exemple de Maersk (leader mondial du transport maritime). Durant une période de 10 jours, l'entreprise a dû revoir l'installation de plus de 4 000 serveurs, 2 500 applications ou encore 45 000 ordinateurs. Un second exemple concerne la centrale nucléaire de Tchernobyl. Cette dernière a été infectée et les répercussions ont été colossales. En effet les mesures de radioactivités ne pouvaient plus être déterminées automatiquement mais manuellement. Comme pour l'incident WannaCry, il est difficile d'évaluer précisément la perte totale. Cependant, elle fut estimée à environ une

dizaine de milliards de dollars ;

- **Covid-19 :** Un accroissement des cyber-incidents a été constaté de par un usage accru des outils numériques ainsi qu'une généralisation du télétravail entraînant un mélange entre outils personnels et outils professionnels. De plus, une campagne d'attaques opportunistes a eu lieu durant ce début de crise sanitaire. En effet, les individus étaient particulièrement vulnérables. C'est pourquoi, d'après la coalition *Cyber-Threat Covid-19*, environ 26 000 URL ou domaines malveillants liés au Covid-19 ont été identifiés durant le mois d'avril 2020. Enfin, une recrudescence de tous types d'attaques classiques a été constatée (comme le fait référence l'article piloté par Khan Navid Ali et al [13]). Un évènement particulièrement marquant concerne les attaques contre les services de santé. Comme il était possible de le constater, durant ces deux dernières années, les hôpitaux ou plus généralement les services de santé ont été mis à rude épreuve de par le nombre de lits réquisitionnés et le manque de moyens/personnels. Ces services saturés ont en plus de cela connu une multitude de cyber-attaques afin d'exploiter au maximum les vulnérabilités détectées ;

- **Colonial Pipeline :** En mai 2021, un système d'oléoduc américain (*Colonial Pipeline*) du Texas a subi une cyber-attaque de type double extorsion (rançongiciel associé à du chantage) forçant un arrêt de la chaîne de production durant plusieurs jours. A cette occasion, Joe Biden (président des États-Unis) a déclaré l'état d'urgence le 9 mai. En effet, l'attaque du système oléoduc américain est la plus grande cyber-attaque contre une infrastructure pétrolière dans l'histoire des États-Unis. Les pirates ont été identifiés comme appartenant au groupe *Darkside*. Les conséquences ont été répercutées directement sur les professionnels et les particuliers. En effet, des pénuries de carburant ont commencé à se produire dans les stations-service. Ce phénomène entraîna une hausse brutale du prix moyen du carburant qui a atteint son plus haut niveau depuis 2014 (environ 3$ le gallon) ;

- **Microsoft Exchange :** Début 2021, Microsoft Exchange a découvert qu'il était victime d'une cyber-attaque. L'outil de messagerie électronique est utilisé par plusieurs centaines de milliers d'entreprises. Les pirates accusés de cette attaque ont exploité une faille *0-day*. Ce type de faille représente une vulnérabilité d'un logiciel qui a toujours été présente (depuis sa création) mais qui n'a jamais été repérée auparavant. Les victimes sont essentiellement les PME, mais également les municipalités, les administrations ou encore les banques ;

- **Guerre Ukraine-Russie :** Le 24 février 2022, les russes ont envahi l'Ukraine. Cette invasion a été opérée militairement parlant (entrée des soldats sur le territoire ukrainien), mais également numériquement (cyber-attaque du réseau satellite KA-SAT). Cette cyber-attaque engendra une perte de communication au début de la guerre. La Russie a tenté de perturber une multitude de moyens de communication comme les communications satellites, les fournisseurs d'accès à internet ou encore les opérateurs mobiles. De ce fait, les forces militaires ukrainiennes ont été empêchées partiellement de communication durant les prémices de la guerre. Au fil des jours, les russes ont principalement ciblé les outils informationnels comme le bombardement de tours de télévisions ou encore les radios. Cependant, aucune attaque de forte sévérité n'a encore eu lieu. Mais, plusieurs milliers d'offensives de faible sévérité ayant pour objectif de saturer les sites internets afin de les rendre inopérant.

1.3 État des lieux du marché français de l'assurance cyber

L'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) a publié en 2021 la première étude exhaustive sur la couverture assurantielle du risque cyber en France : l'enquête LUCY (LUmière sur la CYberassurance) pilotée par Philippe Cotelle [7] , administrateur et président de la commission Systèmes d'Information de l'AMRAE, vice-président de FERMA et Risk Manager d'Airbus Defence & Space. Les données utilisées lors de cette étude proviennent des courtiers. Cependant, ces derniers ne précisent pas explicitement si les sinistres enregistrés se déroulent sur le territoire français ou à l'étranger. C'est pourquoi, une grande attention devra être portée tant aux chiffres présentés qu'à la sur-interprétation qu'il est possible d'en faire.

Dans cette enquête et à l'aide du graphique ci-dessous, une augmentation du volume des primes d'assurance cyber a été constatée. En effet, en 2019, ce volume était de 87 millions d'euros contre 130 millions d'euros en 2020 soit une hausse de 49%. En revanche, les indemnités versées (sinistres) ont cru drastiquement comparé à la hausse des primes. En 2019, le volume de sinistres était de 73 millions d'euros contre 217 millions d'euros en 2020 soit une hausse de 297%.

Du point de vue des assureurs, en comparant le ratio sinistres sur primes (S/P), il valait 84% en 2019 contre 167% en 2020 soit une hausse de 83 points de pourcentages en l'espace d'une année. À cause des résultats précédents, les entreprises bénéficient de réductions de garanties tout en ayant un tarif qui augmente. Le problème proviendrait principalement d'une inflation qui a été créée par le biais de quelques sinistres de fortes sévérités. Sans ces derniers, les résultats techniques de l'année 2020 auraient été semblables à ceux de l'année antérieure.

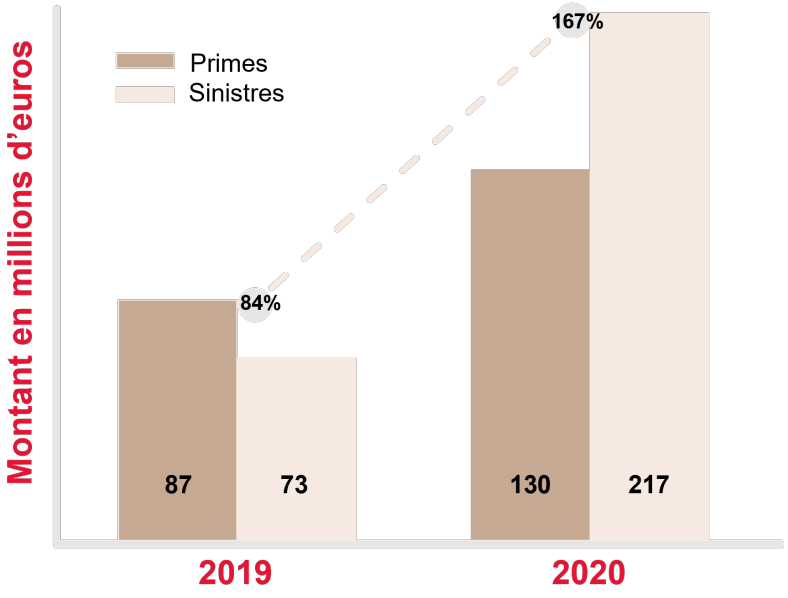

FIGURE 1.3 – Évolution de la sinistralité

Le rapport fait également l'état des lieux suivant : selon l'AMRAE, environ 87% des grandes entreprises (sur un panel de 287 recensées par l'INSEE) seraient couvertes à l'aide d'un contrat de cyber-assurance mais pour une couverture qui ne concorde pas avec leur niveau

d'exposition. Cette sous-assurance provient du fait qu'il est difficile d'évaluer à la juste valeur les coûts de gestion, le risque de réputation ou encore les frais en cas de pertes de données.

Le volume global des primes ne permet pas de faire face à des sinistres de forte sévérité. Néanmoins, ce volume permettrait de faire face à des sinistres de faible intensité. Selon Philippe Cotelle, plus de $\frac{4}{5}^{eme}$ du volume des primes en cyber assurance proviendrait des grandes entreprises. Par conséquent, une sous-assurance de la part des ETI (Entreprises de Taille Intermédiaire), des PME (Petites et Moyennes Entreprises), des TPE (Très Petites Entreprises) ainsi que des collectivités publiques a été remarquée. En prenant l'exemple des ETI, seulement 8% d'entre elles auraient souscrit une assurance cyber en 2020 (soit 441 entreprises sur un panel de 5 763). Les 92% restant ont pu décider de s'auto-assurer par la mise en place d'une captive ou ont pu souscrire une police responsabilité civile intégrant une garantie cyber voire même de ne pas s'assurer entièrement. Ces chiffres seraient cohérents du fait de l'ampleur qu'un sinistre cyber peut provoquer. En effet, une grande entreprise de plusieurs milliards d'euros aura un coût marginal d'arrêt total d'activité largement supérieur à celui d'une ETI ou d'une PME. C'est pourquoi, ce type d'entreprise a tout intérêt à souscrire une assurance cyber. Néanmoins, une certaine prise de conscience a lieu ses dernières années. Les ETI ont certes un taux de couverture très bas mais ont connu une croissance de souscription d'assurance cyber d'environ 44% en 2020 selon l'AMRAE. Il en va de même pour le PME avec un chiffre avoisinant les 17%.

Selon la FFA, il est possible d'observer à l'aide du diagramme ci-dessous que le marché est porté essentiellement par les grandes entreprises. En effet, sur le volume total des primes d'assurance cyber qui ont été payées en 2020, environ 82% de ces dernières proviennent des grandes entreprises contre 6% envers les PME et TPE. Une autre remarque a été effectuée à propos des collectivités publiques qui peinent à s'équiper d'une assurance cyber : seulement 1% d'entre elles ont souscrit à cette assurance. Néanmoins, n'oublions pas que ces chiffres ne tiennent pas compte des éventuelles garanties cyber que pourraient détenir les entreprises ainsi que les collectivités.

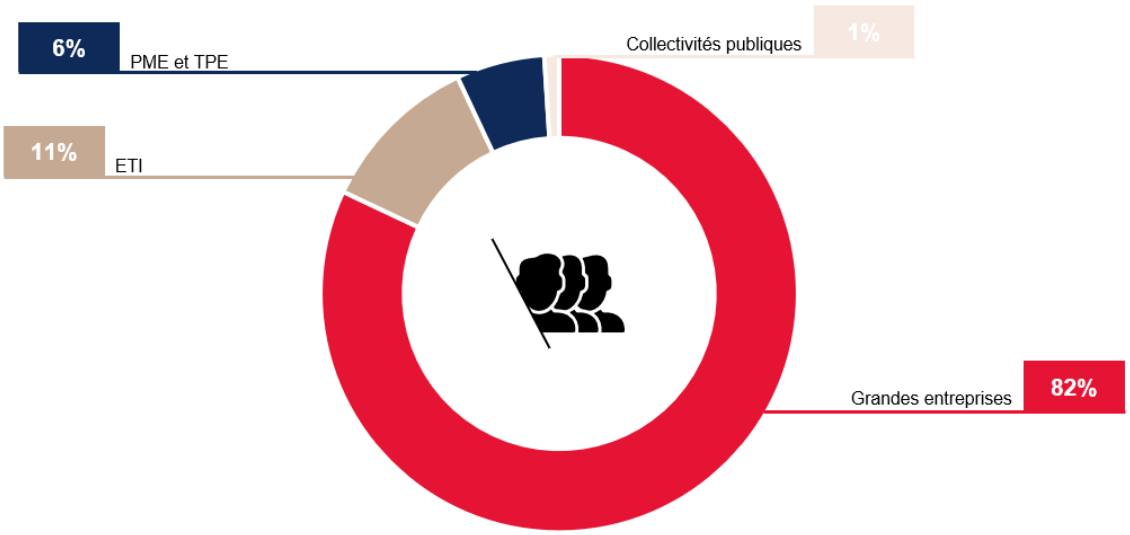

FIGURE 1.4 – Répartition des primes d'assurance cyber en 2020 selon la FFA

La volatilité des sinistres cyber engendre, toute chose égale par ailleurs, une forte variation

des S/P. En effet, en prenant l'exemple de 2019, aucun sinistre de très forte sévérité (entre 10 et 40 millions d'euros) n'aurait été déclaré par les grandes entreprises. Mais en 2020, 4 sinistres l'auraient été. Cette fluctuation engendre donc une variation importante du ratio sinistres sur primes passant de 44% en 2019 à plus de 190% en 2020 pour les grandes entreprises. A l'aide du graphique ci-dessous, il est possible d'observer une certaine stabilité pour les sinistres de faible, moyenne et grande sévérités entre 2019 et 2020 mais une instabilité pour les sinistres de très forte sévérité. Cependant, ces chiffres ne sont pas à prendre mot comptant car il est difficile de donner une tendance avec seulement 2 années d'historique.

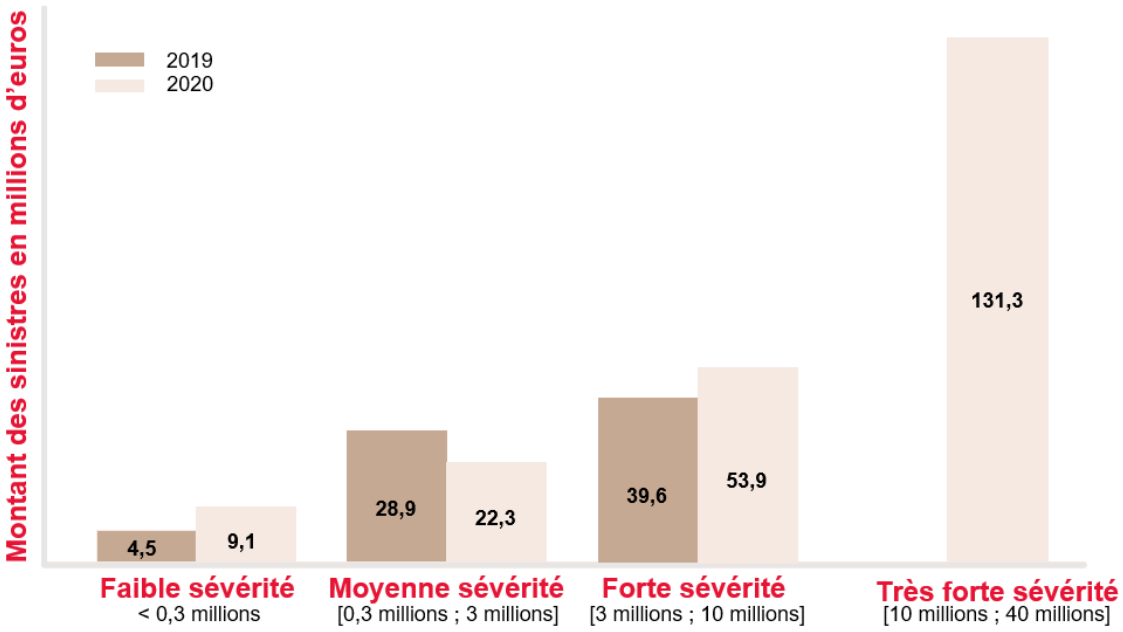

FIGURE 1.5 – Comparaison des sinistres entre 2019 et 2020 selon le degré de sévérité d'après l'étude LUCY de 2021

TABLE 1.1 – Fréquence des sinistres selon leur gravité

		Gravité des sinistres			
Taille	Année	XS & S (0-300k)	M & L (300k-3M)	XL (3M-10M)	XXL (10M-45M)
GE	2019	84,90%	9,60%	5,50%	0,00%
GE	2020	73,25%	15,05%	7,00%	4,70%
GE	Moyenne	79,07%	12,33%	6,25%	2,35%
ETI & PME	2019	75,03%	21,00%	3,70%	0,00%
ETI & PME	2020	89,80%	9,10%	1,10%	0,00%
ETI & PME	Moyenne	82,55%	15,05%	2,40%	0,00%

D'après le tableau précédent, l'AMRAE fait le constat suivant : environ $\frac{3}{4}$ des sinistres cyber représentent un coût de gravité XS & S (0-300k) pour les grandes entreprises. Quant au ETI & PME, environ 8 sinistres sur 10 sont de faibles sévérités. L'enquête LUCY permet donc de mettre en évidence que la plupart des sinistres cyber sont de faible sévérité. De plus, nous remarquons également que les sinistres inférieurs à un coût de 10M sont stables

entre 2019 et 2020. Quant aux sinistres XXL, seul les grandes entreprises ont connu en 2020 ce type de sinistralité représentant un coût de dommage entre 10M et 45M.

Le manque de données sur la cyber assurance représente un frein au développement de modèle économique permettant d'évaluer de manière juste les garanties des contrats. Une des solutions que pourraient apporter les assureurs est la mutualisation grâce à une augmentation du nombre d'assurés ainsi qu'un historique de données complet. Néanmoins, le rapport indique également que nous assistons aujourd'hui à un changement brutal des polices cyber qui voient leur niveau de franchises, leur capacité ainsi que leur taux varier drastiquement. Les entreprises ainsi que les collectivités seraient assez réticentes à ces changements d'une part mais également avec un contexte économique et sanitaire qui arrive à saturation. Il faudrait néanmoins différencier la situation des grandes entreprises où l'offre serait assez peu développée comparé à la demande, à la situation des ETI, PME et TPE qui bénéficieraient d'un marché concurrentiel mais auraient tendance à méconnaître et sous-estimer les répercutions du risque cyber.

Outre le rapport LUCY de l'AMRAE, plusieurs autres acteurs ont également réalisé plusieurs études comme celles proposées par :

- Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) en janvier 2022. Le CESIN publie annuellement un rapport sur la cyber-sécurité [6]. Nous pouvons également trouver dans cette étude une partie sur la cyber-assurance. Cependant, il y a un biais dans cette étude qu'il faut quand même souligner : la faible part de PME (à peine 300 ici) dans le périmètre ;
- Le rapport de l'ANSSI [2] sur la menace rançongicielle en janvier 2021 ;
- La FFA avec la rédaction d'un livre blanc intitulé « Bâtir une économie de la donnée innovante et protectrice en faveur des Français »[16]. Lors de cette étude plusieurs propositions ont été faites afin d'améliorer la connaissance du risque cyber auprès de tous. Les propositions sont les suivantes :
  - « Inclure une sensibilisation aux risques cyber dans le parcours des jeunes élèves (primaire, collège, lycée) sous l'égide du ministère de l'Éducation Nationale, de la Jeunesse et des Sports, sur le modèle des actions de la Prévention routière ;
  - Clarifier la position de l'État français et de l'Union européenne sur la légalité de l'assurabilité du remboursement des rançons dans le cadre de cyberattaques pour encadrer leurs paiements ;
  - Développer une culture des risque cyber au sein des entreprises et des collectivités territoriales afin d'accélérer la résilience cyber de l'économie française et de permettre le développement des couvertures assurantielles ;
  - Amplifier les efforts de sensibilisation spécifique auprès des TPE-PME, principales cibles des attaques cyber pouvant servir de porte d'entrée pour cibler les grands groupes dans le cadre de relations de sous-traitance ;
  - Mettre en place au niveau européen un cadre ouvrant l'accès aux données des véhicules connectés et qui les sécurise, c'est-à-dire un dispositif qui garantisse le respect de deux principes clés : le libre choix de l'utilisateur de partager ou non ses données ainsi que l'accès transparent et équitable pour tous les acteurs ;
  - Rendre éligibles à l'apprentissage les compléments de formation pour des compétences numériques et renforcer l'accompagnement des salariés de l'assurance dans un contexte de digitalisation des activités. »

1.4 Revue juridique

Afin d'appréhender la difficulté législative qui accompagne le risque cyber, Valéria Faure Muntian [10] (ex-députée de la Loire et présidente du groupe d'études assurances de l'Assemblée Nationale) a rédigé un rapport évoquant les principaux problèmes que rencontrent le gouvernement lors de la mise en place de règles communes et y présente plusieurs solutions.

Aujourd'hui, il n'existe toujours pas d'interdiction formelle pour les assureurs d'indemniser l'assuré victime d'un rançongiciel dans le cadre d'une police d'assurance cyber. En effet, selon l'article 421-2-2 du code pénal, « Constitue également un acte de terrorisme le fait de financer une entreprise terroriste en fournissant, en réunissant ou en gérant des fonds, des valeurs ou des biens quelconques ou en donnant des conseils à cette fin, dans l'intention de voir ces fonds, valeurs ou biens utilisés ou en sachant qu'ils sont destinés à être utilisés, en tout ou partie, en vue de commettre l'un quelconque des actes de terrorisme prévus au présent chapitre, indépendamment de la survenance éventuelle d'un tel acte ». Ainsi, plusieurs acteurs ont été monopolisés afin d'étudier la question de la légalité envers l'assurabilité de l'indemnisation des rançons. Les acteurs sont multiples et permettent une pluralité de réflexions comme le Haut Comité Juridique de la Place Financière de Paris missioné par le Ministère de l'Économie et des Finances ainsi que la Fédération française de l'assurance (FFA), l'ACPR ou encore des professionnel du droit (avocats, magistrats, professeurs).

Contrairement à la France, les États-Unis ont une vision ferme sur la question. Le Trésor américain a prononcé en 2020 une volonté de punir les entreprises qui paieraient une rançon suite à un rançongiciel. Une volonté commune est en train de naître en France et a pour vocation d'inscrire dans la loi l'interdiction pour les assureurs de garantir, couvrir ou d'indemniser la rançon et se porter davantage vers la prévention, l'accompagnement et l'assurance des conséquences pour une entreprise. Cependant, à l'heure actuelle en France, aucune interdiction formelle concernant l'indemnisation des rançongiciels n'a été faite. C'est pourquoi, plusieurs propositions ont été faites par la FFA (détaillées précédemment) permettant d'accompagner les acteurs ainsi que de développer les connaissances du risque cyber aux yeux de tous.

Depuis plusieurs années, la législation a beaucoup évolué et a conduit la création d'une multitude d'autorité. Certaines ont été crée dans le but de faire face directement au risque cyber tandis que d'autres permettent de réguler plus généralement les données :

- AFA (Agence Française Anticorruption) : elle a pour objectif d'aider les personnes morales ou physiques confrontées à prévenir et à détecter les atteintes à la probité ;
- CNIL (Commission Nationale de l'Informatique et des Libertés) : elle est le régulateur des données personnelles. Elle accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits.

La création des autorités ci-dessus permet de prévenir, gérer et résoudre les conflits que les personnes morales et les particuliers peuvent rencontrer. Une volonté de régularisation de l'utilisation des données naquit. Afin de répondre à ce besoin et d'apporter des protections supplémentaires, le Règlement Général sur la Protection des Données (RGPD) a été élaboré. Il définit les règles sur la manière de collecter et d'exploiter les données. Parallèlement

à la mise en place d'une réglementation dédiée à la protection des données personnelles, d'autres législations visent également plus de transparence vis-à-vis des consommateurs et partent du principe qu'une bonne protection des données, c'est avant tout une bonne organisation des données au sein de l'entreprise et une bonne maîtrise de son utilisation. Ainsi et parallèlement au RGPD, deux autres contextes normatifs majeurs sont à signaler :

- La DDA (Directive sur la Distribution d'Assurance) ;
- L'organisation de la qualité des données au sein de l'entreprise.

Le Règlement Général sur la Protection des Données est le successeur de différentes lois nationales et européennes remontant jusqu'à la loi Informatique et Libertés de 1978. La création du RGPD a été retracée à l'aide de la frise chronologique ci-dessous :

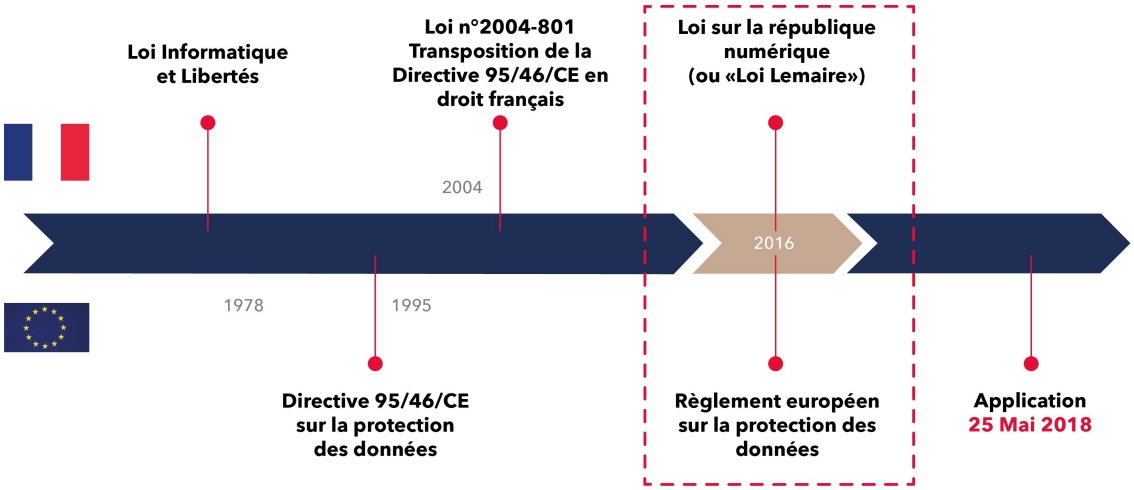

FIGURE 1.6 – Mise en place du RGPD

Le Règlement Général sur la Protection des Données (RGPD) s'applique uniformément à tous les pays de l'Union Européenne depuis mai 2018. Le Règlement vise à protéger les données à caractère personnel. Il a pour objectifs de renforcer les droits des personnes, responsabiliser les acteurs traitant des données ainsi que de renforcer la coopération avec le régulateur.

En cas de négligence dans la protection des données personnelles, un acteur peut s'exposer aux risques suivants :

- Risque financier : l'assureur peut être condamné à payer des amendes beaucoup plus lourdes que dans le passé. Le règlement européen prévoit des sanctions qui peuvent aller de 2% à 4% des revenus annuels selon la gravité des failles. De plus, toute atteinte à la protection des données pourra donner lieu aussi à des réparations vis-à-vis des adhérents ;
- Risque opérationnel : un arrêt temporaire de l'activité peut être imposé le temps de la mise en conformité des mesures de protection ;
- Risque d'image : l'éventuelle médiatisation du non-respect peut porter atteinte à l'image de l'assureur.

Afin de défendre l'assurabilité du risque cyber, certains parties utilisent l'article L. 113-1 du code des assurances évoquant le fait que l'assuré est assurable dès lors que ce dernier est victime d'une faute intentionnelle ou non commise par un tiers. De plus, l'article L. 121-2 de ce même code indique le fait que l'assureur est garant des dommages et pertes causés par un tiers dont l'assuré est civilement responsable. Selon Valéria Faure-Muntian, il est recommandé d'autoriser la couverture et la prise en charge des amendes administratives par l'assureur.

Le gouvernement a mis en place plusieurs services permettant de lutter contre la cyber-criminalité. Prenons l'exemple du site internet sur la cyber-malveillance lancé par l'ANSSI et le Ministère de l'Intérieur en 2017. Cette plateforme permet d'accompagner les victimes de cyber-attaques. Plusieurs groupes ont également été crées afin de lutter contre cette criminalité au sein de la gendarmerie, mais également avec le Ministère de l'Économie et des Finances ainsi qu'avec le Ministère de la Justice, le procureur de la République, le pôle de l'instruction, le tribunal correctionnel et la cour d'assises de Paris. Néanmoins, les dossiers sont de plus en plus nombreux et complexes. Le Code pénal ne serait plus aussi efficace face à la cyber-criminalité. Par ailleurs, le parquet rencontre de plus en plus de difficultés liées à l'obtention et à la validité des preuves numériques ainsi qu'un manque de ressources humaines et matérielles permettant un suivi adéquat.

Les garanties proposées dans un contrat cyber varient d'un assureur à l'autre. En effet, cela pourrait être expliqué d'une part avec une mauvaise connaissance du risque mais également avec une mauvaise estimation des coûts des sinistres. Pour autant, le rapport de l'Assemblée Nationale a donné un exemple de garanties proposées dans un contrat d'assurance cyber :

- Assistance et gestion de crise :
  - Un expert informatique est démarché pour déterminer la cause et l'étendue de l'attaque. Il détermine également la capacité de l'assuré à éviter ce futur incident ;
  - Un avocat détermine s'il peut appliquer la loi sur la Notification. Il aide également l'assuré lors d'une violation d'un contrat marchand et de récupération des coordonnées bancaires ;
  - Notification aux individus s'étant fait violer leurs données personnelles ;
  - Surveillance sur Internet sur les apparitions des données personnelles qui ont pu être volées ;
- Responsabilité civile : L'assurance prend en charge les conséquences pécuniaires et les frais de défense si l'assuré a subi :
  - Atteinte aux données ;
  - Atteinte aux systèmes ;
  - Non-respect d'une charte de protection des données ;
- Responsabilité liée au contenu d'un site internet : L'assurance prend en charge les conséquences pécuniaires et les frais de défense si l'assuré a subi :
  - Diffamation, injure, atteinte à la réputation ;
  - Atteinte au respect de la vie privée et au droit d'image ;
  - Appropriation illégale d'un nom ou d'une image dans un but commercial ;
  - Plagiat, piratage ;
  - Contrefaçon d'un droit d'auteur (nom de domaine, logo, metatag) ;

- Usage d'un hyperlien en profondeur ou framing d'un contenu internet ;

◦ Relations publiques : L'assurance paie les consultants en gestion de crise, la diffusion de messages publics ;

◦ Enquêtes administratives : L'assurance paie les frais de défense liés à la réclamation auprès de la CNIL (et des CNIL étrangères) lors d'une cyber-attaque ;

◦ Pénalités PCI-DSS : sont prises en charge par l'assurance ;

◦ Cyber extorsion (rançongiciels) : l'assurance prend en charge :

- Tout paiement ou toute remise de biens fait sous la contrainte, par ou pour le compte de la société souscriptrice ;
- Toute perte, destruction, disparition des espèces et biens en cours de transfert alors qu'ils seraient convoyés par toute autre personne autorisée par ou pour le compte de la société souscriptrice à cette fin ;
- Les frais et honoraires payés par ou pour le compte de la société souscriptrice à des consultants en sécurité ;

◦ Reconstitution des données : L'assurance prend en charge les frais de reconstitution des données si :

- Altération, infection, destruction, suppression ou endommagement d'une donnée protégée ;
- Incapacité d'accéder à une donnée protégée ;

◦ Perte d'exploitation : L'assurance prend en charge les pertes de revenus et dépenses supplémentaires au cours d'une période d'interruption (pas au-delà de 60 jours) de l'assuré lors d'une cyber-attaque. (Cette clause ne fonctionne pas si le sinistre dépend d'une responsabilité envers un tiers).

1.5 Gestion du risque cyber : modélisation actuelle

Le risque cyber a des conséquences multiples impactant la production ou encore l'image. Il ne peut donc pas être complètement transféré à l'assureur. Comme abordé précédemment, la couverture financière est insuffisante. Les contrats de responsabilité et de dommage que nous connaissons ne sont pas adaptés à ce risque. Déterminer la tarification d'une garantie cyber ou plus généralement d'une garantie classique réside dans le fait de surmonter l'inversion du cycle de production ainsi que l'asymétrie d'information.

Dans le contexte d'assurance cyber, l'assuré ne connaît pas forcément plus son risque que l'assureur. Prenons l'exemple d'une grande entreprise et d'une TPE. La première aura sûrement un service composé d'experts capables d'évaluer l'exposition de l'entreprise, la robustesse des logiciels et les éventuelles vulnérabilités alors que la TPE aura beaucoup plus de difficultés à les évaluer.

Le but premier serait d'analyser le risque cyber à l'aide d'un portefeuille sur lequel l'historique est faible. La moindre calibration se fera avec une précision faible car le nombre de données n'est pas assez conséquent pour obtenir des résultats robustes. Un moyen de contourner ce problème serait de se procurer une base de données de référence. Néanmoins, la population présente dans le portefeuille ne se comporte pas toujours comme la population de référence, introduisant un biais dans l'analyse.

Durant plusieurs années, la tarification en assurance cyber était fondée dans la majeure partie en fonction de la concurrence. Néanmoins, au vu des prestations et des cotisations versées, les primes d'assurances se trouvent très volatiles d'une année à l'autre. C'est pourquoi, plusieurs auteurs ont analysé ce risque afin d'apporter une meilleure compréhension sur les coûts qu'il encourt.

1.5.1 Modèles généraux sur le risque cyber

Plusieurs analyses transversales ont été menées afin d'analyser au mieux le risque cyber :

- L'analyse du risque cyber comme un risque extrême : utilisation de la théorie des valeurs extrêmes (Olivier Lopez et al [15]) ;
- Modélisation et prévision de la fréquence des cyber-attaques à l'aide du processus de Hawkes (Caroline Hillairet et al[11]) ;
- L'étude de la propagation des sinistres cyber à travers un portefeuille : application aux processus de comptage et modèle épidémiologique (Olivier Lopez et Caroline Hillairet [14]).

L'analyse du risque cyber comme un risque extrême : utilisation de la théorie des valeurs extrêmes

Ces travaux ont été menés en 2020 par Olivier Lopez (professeur à Sorbonne Université et directeur de l'ISUP), Sébastien Farkas (doctorant à Sorbonne Université) et Maud Thomas (maître de conférences à Sorbonne Université et co-présidente du Master Actuariat de l'ISUP).

Dans cet article, les auteurs proposent de séparer le comportement extrême en utilisant la théorie des valeurs extrêmes pour modéliser à l'aide des arbres de classification des groupes homogènes. Ceci permettra de déterminer un niveau maximal des garanties que l'assureur pourrait proposer à l'assuré dans sa police d'assurance ainsi qu'une tarification. Pour ce faire, les auteurs rappellent que les variables aléatoires de fortes sévérités n'ont pas d'espérance. Il est donc difficile d'évaluer le coût moyen associé. Une façon de contourner le problème serait d'exclure ces risques en mettant une limite d'indemnisation à la police. Cependant, le problème ne sera pas pour autant écarté entièrement puisque la difficulté sera de fixer cette limite dans le cas d'une queue de distribution lourde. Le phénomène qui apparaît est le suivant : plus le cyber évènement sera sévère, plus la limite sera basse afin de se protéger au mieux du risque mais cela détériorera la garantie. Sur ces risques, nous constatons un manque de données et d'informations historiques.

Les auteurs ont donc décidé d'étudier la queue de distribution à l'aide de la théorie des valeurs extrêmes. L'indice de queue de distribution a permis de déterminer si l'évènement est assurable ($\gamma < 1$) ou non ($\gamma > 1$). Néanmoins, le fait de mélanger risque assurable et non assurable vient biaiser l'analyse du fait de la grande hétérogénéité des cyber évènements. En effet, nous aurions tendance à surestimer davantage les risques non assurables car le phénomène le plus sévère viendrait écraser les autres phénomènes.

Une alternative proposée a été de déterminer des classes de sinistres et d'assurés sur lesquelles des hypothèses seront portées. Les auteurs ont modélisé cette étude à l'aide de la base de données PRC. Dans cette dernière (que nous étudierons plus en détail dans la suite du mémoire), la variable coût n'est pas présente. Néanmoins, il est possible de

l'estimer à l'aide de la variable volume de données touchées. Ce lien a été proposé par Jacobs [12] puis actualisé par les auteurs et se présente de la façon suivante :

$$logL = 9,59 + 0,57\ logY,$$

où L représente le coût d'un sinistre cyber et Y représente la sévérité de l'attaque.

De ce fait, il est maintenant possible d'établir un lien entre l'indice de queue de L (γ_L) et celui de Y (γ_Y) :

$$\gamma_L = 0,57\gamma_Y$$

La méthodologie suivie a été de mettre en lien les techniques de data science et notamment les arbres de régression avec la théorie des valeurs extrêmes. L'idée générale est la suivante : comme vu précédemment, considérer tous les sinistres au global rendra la queue de distribution très lourde du fait des sinistres de forte sévérité.

Après regroupement des classes de sinistres, deux arbres de régressions ont été réalisés lors de l'étude. Le premier permet d'analyser les sinistres se situant en milieu de distribution. Chaque noeud de l'arbre correspond à une variable de la base de données. En fonction des valeurs de cette dernière, il est possible de se déplacer d'une branche à une autre. A la fin de cette classification, nous retrouvons un regroupement des types d'incidents et d'assurés dans chacune des feuilles de l'arbre avec une évaluation du risque associé. Quant au second arbre, il permet l'étude des sinistres « non acceptables » sur la queue de distribution. Nous remarquons que les variables présentes dans les noeuds ne sont pas les mêmes qu'avec l'arbre précédent. Dans cet arbre, l'indice de queue global est supérieur à 1 mais en vérité plus de 80% des sinistres ont un gamma proche voire plus petit que 1.

L'intérêt d'une telle modélisation est non pas de mélanger tous types de sinistres mais plutôt de faire la distinction selon des critères définis préalablement (sévérité, typologie, ...).

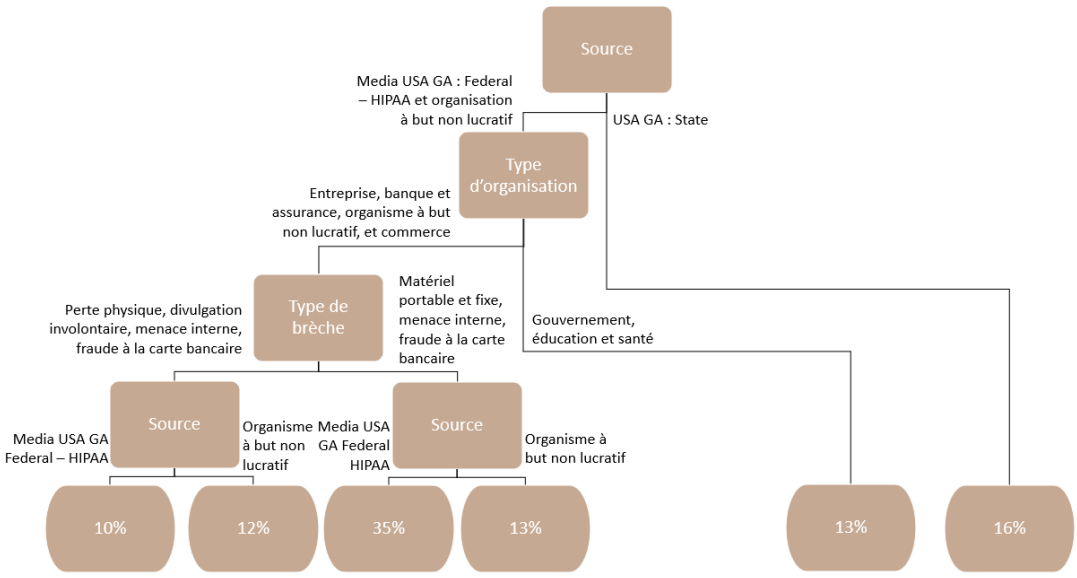

FIGURE 1.7 – Analyse de la distribution centrale à l'aide d'un arbre médian

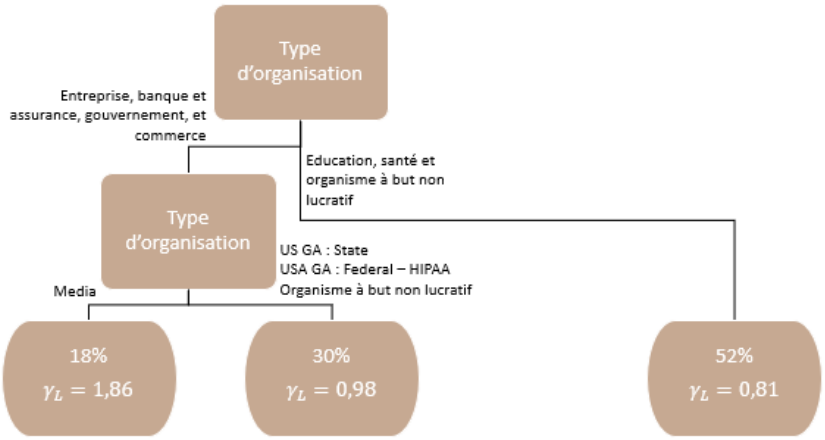

FIGURE 1.8 – Analyse de la distribution à l'aide d'un arbre de régression d'une pareto généralisée

A l'issue de cette étude, les auteurs ont pu déterminer un niveau maximal des garanties que l'assureur pourrait proposer à l'assuré dans sa police d'assurance ainsi qu'un modèle de tarification simple.

Modélisation et prévision de la fréquence des cyber-attaques à l'aide du processus de Hawkes

Ces travaux ont été menés en 2020 par Caroline Hillairet (professeur à l'ENSAE Paris, responsable du master d'actuariat et membre du CREST, Laboratoire de Finance et d'Assurance), Alexandre Boumezoued (Directeur R&D chez Milliman) et Yannick Bessy-Roland (Actuaire IA).

Dans cet article, les auteurs proposent un cadre multivarié du processus de Hawkes pour modéliser et prédire la fréquence des cyber-attaques. Le cadre multivarié a été retenu afin de modéliser l'autocorrelation, l'excitation et la contamination entre les évènements cyber. Une approche à l'aide d'un processus de poisson ne peut être réalisée. En effet, l'intensité d'arrivée des évènements doit prendre en compte le passé. Afin de palier cela, les auteurs ont décidé d'utiliser un processus de Hawkes multivarié permettant de modéliser l'intéraction entre le type d'entités, d'attaques et d'états. Pour cela, il faut tenir compte de l'auto et de l'inter-excitation du processus de saut. L'auto-excitation est définie comme le fait que chaque évènement croît la probabilité pour un nouveau évènement de se produire dans un groupe et l'inter-excitation comme le fait que chaque attaque dans un groupe augmente la probabilité d'occurrence de nouveaux événements dans les autres groupes.

En supposant que K groupes homogènes ont été constitués et en notant $\left(\tau_n^{(i)}\right)_{n\geq 1}$ le temps de sauts du i-ème groupe (temps avant la survenance du sinistre i avec $1 \leq i \leq K$). Alors ils définissent la forme de l'intensité de l'arrivée d'un sinistre dans un groupe i comme :

$$\lambda_i(t) = \mu_i + \gamma_i t + \sum_{j=1}^{K} \sum_{\tau_n^{(j)} < t} \alpha_{i,j} exp\Big(- \beta_i (t - \tau_n^{(j)}) \Big)$$

Cette intensité peut se décomposer en deux partie :

- $\mu_i + \gamma_i t$ représente l'intensité de base qui ne prend pas en compte l'auto-excitation. Elle représente la probabilité qu'un cyber évènement arrive de façon non excitée par un évènement arrivé précédemment ;
- $\sum_{j=1}^{K} \sum_{\tau_n^{(j)} < t} \alpha_{i,j} exp\Big(- \beta_i (t - \tau_n^{(j)}) \Big)$ représente l'impact des évènements passés faisant augmenter l'intensité d'arrivée d'un évènement dans le groupe i.

La représentation graphique est la suivante : chaque saut correspond à la survenance d'un cyber évènement faisant croître l'intensité du processus. De plus, il est remarqué également qu'en période de non sinistre, l'intensité décroît de façon exponentielle car le noyau d'excitation présent dans la formulation de l'intensité correspond à un noyau exponentiel. En supposant deux groupes, le graphique se présente comme ci-dessous.

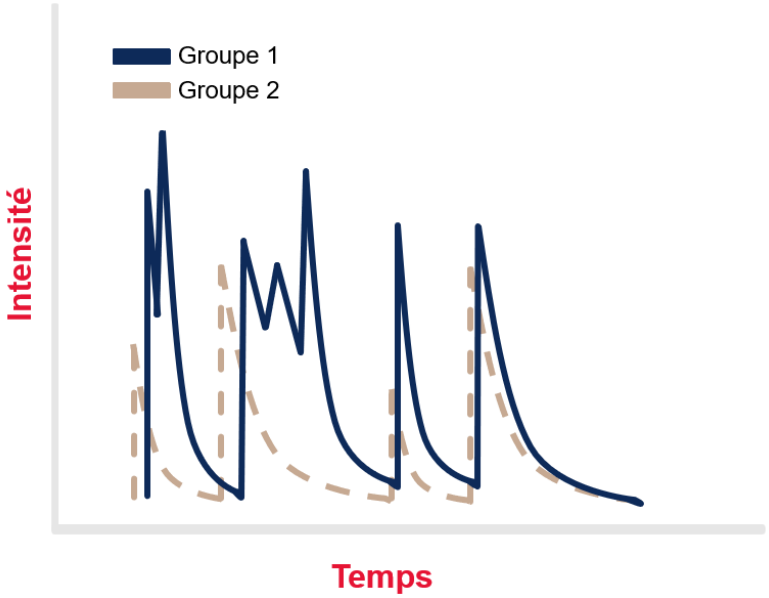

FIGURE 1.9 – Intensité du processus de Hawkes pour deux groupes

Les auteurs remarquent également que le groupe 2 est seulement excité par lui même. En effet, le groupe 1 n'a aucune influence sur le groupe 2. A l'inverse, le groupe 1 est influencé par le groupe 2.

Il est possible de retranscrire ces informations à l'aide du coefficient $\alpha_{i,j}$ représentant l'impact du groupe j sur le groupe i. Dans cette exemple, la matrice d'inter-excitation s'exprime de la façon suivante :

$$\alpha = \begin{pmatrix} \alpha_{1,1} & \alpha_{1,2} \\ \alpha_{2,1} & \alpha_{2,2} \end{pmatrix} = \begin{pmatrix} 0 & c_1 \\ 0 & c_2 \end{pmatrix} \text{ avec } c_1, c_2 \text{ des constantes.}$$

Le point retenu lors de l'étude est l'effet de regroupement des données. En effet, certaines périodes étaient fréquemment touchées par des cyber-attaques et d'autres peu. Afin de calibrer au mieux les paramètres du processus, différents groupes ont été formés en fonction du secteur d'activité de l'organisation. Cette étude aura permis de déterminer la fréquence de sinistres et d'étudier l'impact de ces derniers entre et à l'intérieur des différents groupes.

L'étude de la propagation des sinistres cyber à travers un portefeuille : modèle épidémiologique

Ces travaux ont été menés en 2020 par Olivier Lopez et Caroline Hillairet.

Les deux modèles précédents permettaient de décrire de façon « classique » la fréquence et la sévérité des cyber-attaques. Une nouvelle étude a été réalisée afin de mettre en évidence les scénarios par accumulation et les conséquences d'une contagion au sein d'un portefeuille. Ce rapport fait notamment référence à l'incident *Wannacry* que nous avons décrit en introduction. En effet, il ne faut pas associer directement une attaque cyber à une victime : les victimes peuvent être multiples. L'approche du modèle peut être découpée en trois étapes majeures :

- L'étude de la dynamique des évènements cyber en temps réel basé sur des modèles épidémiologiques. Le but principal consistait à simuler une trajectoire de contamination d'évènement cyber comme l'incident *Wannacry* ;
- L'étude de l'impact sur un portefeuille d'assurance ;
- La réponse stratégique : déterminer les mesures qui peuvent être prises afin de minimiser le coût des sinistres et le nombre de victimes.

L'approche menée par les chercheurs consistait à répliquer l'analyse de survie à la chronologie des évènements cyber. Ci-dessous, nous retrouvons la représentation de deux polices d'assurances (j et k) qui se font infecter par un évènement cyber.

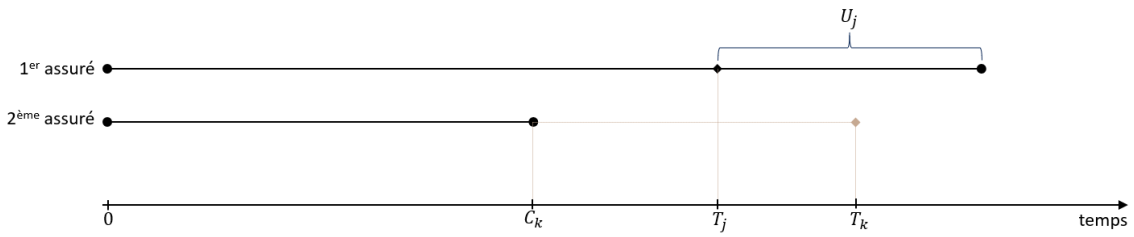

FIGURE 1.10 – Chronologie de deux polices en cas d'une cyber-attaque

Rappelons les notations suivantes :

- T_j : temps d'infection de la compagnie j ;
- U_j : durée d'assistance requis par j ;
- C_j : période durant laquelle l'assuré j arrive à se protéger lui même.

Le premier assuré se fait infecter au temps T_j et va être assisté pendant une durée U_j jusqu'à ce que la crise soit résolue. Nous parlons alors d'assistance immédiate car les réparations sont immédiates et non différées. En effet, après une crise, les indemnisations des dommages peuvent durer très longtemps en cas d'attaque cyber (plusieurs mois voire années). Le second assuré, quant à lui, est capable de se protéger lui même en temps C_k avant l'infection qui aura lieu en T_k si aucune solution n'a été trouvé pour enrayer la contagion. En utilisant ce genre de modèle, l'étude a permis d'avoir une meilleure compréhension de la cyber-épidémie.

La suite de l'étude consista à utiliser le modèle épidémiologique SIR (*Susceptible Infectious Recovered*). Les assurés se font infecter à un taux d'infection β et se rétabliront à un taux

de guérison γ. Les auteurs modélisent alors la viralité de l'attaque de la façon suivante :

$$R_0 = N \times \frac{\beta}{\gamma}$$

où N représente la population. Si $R_0 < 1$, alors l'individu infecté contamine moins d'un autre individu en moyenne, ce qui signifie que l'attaque ne se propage pas et disparaît à terme. À l'inverse, si $R_0 > 1$, alors l'attaque se propage dans la population et devient une cyber-épidémie.

Le but de la modélisation est de contrôler le nombre d'assurés infectés à l'aide de plusieurs scénarios sur les lois selon le degré de réactivité à la crise. Les auteurs concluent alors que la réactivité est un élément crucial dans le contrôle de l'attaque.

1.5.2 Mesure de l'exposition

L'augmentation exponentielle des vulnérabilités est liée d'une part à une standardisation de l'utilisation des logiciels et des sites internet mais également à une croissance pérenne des besoins de notre société. Aujourd'hui, il n'est toujours pas possible d'utiliser des ressources informatiques sans être exposé au risque cyber.

Avant d'aller plus loin, distinguons les notions de vulnérabilité, attaque et intrusion que nous utiliserons dans le cadre de ce mémoire. Ces définitions proviennent du projet MAFTIA rédigé par Powel et al [17] :

- La vulnérabilité est définie comme une faute accidentelle ou intentionnelle, malveillante ou non, dans les spécifications, la conception ou la configuration du système, ou dans la manière dont il est utilisé. La vulnérabilité peut être exploitée afin de créer une intrusion ;
- Une attaque est une faute d'interaction malveillante visant à violer une ou plusieurs propriétés de sécurité. C'est une faute externe créée avec l'intention de nuire. Une attaque peut être ou non réalisée par des outils automatiques ;
- Une intrusion est définie comme une faute malveillante interne, mais d'origine externe, résultant d'une attaque qui a réussi à exploiter une vulnérabilité.

Comme il est possible de s'y attendre, les vulnérabilités des logiciels existent en masse. Néanmoins, certaines sont plus connues et dangereuses que d'autres. Une volonté de classification des vulnérabilités a vu le jour. Aujourd'hui, plusieurs bases de données publiques répertorient les vulnérabilités avec une mesure associée indiquant leur niveau d'importance :

- CVE (*Common Vulnerabilities and Exposures*) ;
- NVD (*National Vulnerability Database*) ;
- VUPEN (*Vulnerability Penetration testing*) ;
- OWASP (*Open Web Application Security Project*) ;
- WASC (*Web Application Security Consortium*).

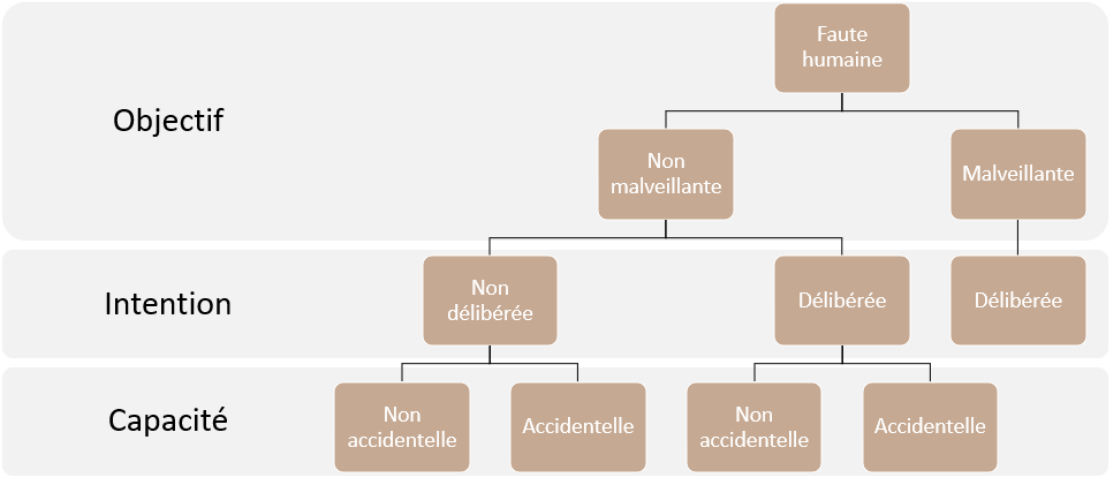

FIGURE 1.11 – Arbre de classification : origine des vulnérabilités

Dans le graphique ci-dessus présenté dans la thèse de Vache-Marconato [19], nous observons que l'origine des vulnérabilités proviendrait de la faute humaine. Celle-ci peut être intentionnelle ou non. Si elle est intentionnelle, la vulnérabilité a forcément été créée délibérément. Néanmoins, si cette dernière a été réalisée dans un but non malveillant, elle peut être dû à une erreur ou simplement une mauvaise décision. Ces deux composantes sont le résultat d'un accident ou d'une incompétence de la part du développeur et/ou de l'utilisateur. Nous pouvons donc conclure que l'intention ainsi que la capacité ont une influence assez faible dans le cas d'une vulnérabilité non malveillante.

En pratique, il est assez difficile d'associer une fréquence de sinistralité à une fréquence de vulnérabilité par manque de données disponible. Néanmoins, il est cependant possible d'associer un indice de risque cyber d'une entreprise à un nombre de sinistres. En effet, l'indice de risque est une mesure plus globale qui est caractérisée par une multitude de variables comme la taille d'une entreprise, le secteur d'activité, la localisation ou encore la présence d'un responsable de la sécurité des systèmes d'information.

Dans le cadre de ce mémoire, nous voudrions créer une mesure temporelle générique qui permette de mesurer le niveau de cet indice de risque et établir le lien avec les sinistres.

L'institut Ponemon a rédigé un rapport en juillet 2021 sur la détermination d'un indice d'exposition aux risques cyber (CRI : *Cyber Risk Index* [18]). Les résultats de l'enquête ont été utilisés afin de créer un indice qui essaie de mesurer la capacité des entreprises à répondre à une multitude de cyber-attaques. Celui-ci est composé de deux indices :

- Indice de cyber-défense (*Cyber preparedness index*) : il représente la capacité d'une organisation à se défendre contre les cyber-attaques ;
- Indice de cyber-menace (*Cyber threat index*) : il représente l'état de la menace au moment où le CRI est calculé.

Le CRI est alors calculé comme la différence entre l'indice de cyber-défense et l'indice de cyber-menace.

Indice de cyber-défense

Un questionnaire composé de 31 affirmations a été élaboré. Celles-ci sont utilisées afin de déterminer la capacité d'une entreprise à faire face aux cyber-évènements. Les réponses sont mesurées à l'aide de l'échelle de variables qualitatives ordinales suivante :

TABLE 1.2 – Notation des questions de cyber-défense

Variables qualitatives	Retranscription quantitative
Fortement en désaccord	0/10
Moyennement en désaccord	2,5/10
Neutre ou indécis	5/10
Moyennement en accord	7,5/10
Fortement en accord	10/10

Afin de déterminer l'indice de cyber-défense, l'institut Ponemon décida de faire une moyenne arithmétique sur la retranscription quantitative en considérant le poids de chaque réponse comme identique.

FIGURE 1.12 – Indice de cyber-défense

TABLE 1.3 – Questionnaire sur la cyber-défense

Affirmations
1. Le budget de sécurité de mon entreprise est suffisant pour protéger les données et l'infrastructure informatique.
2. Le personnel chargé de la sécurité informatique de mon entreprise dispose de connaissances, de compétences et d'une expertise suffisantes pour protéger les bases de données et l'infrastructure informatique.
3. Les dirigeants de mon entreprise considèrent la sécurité informatique comme une priorité absolue.
4. Le responsable de la sécurité informatique de mon entreprise rend des comptes à la direction générale (comme le PDG, le directeur d'exploitation ou le directeur de l'information).
5. Le directeur général et le conseil d'administration de mon entreprise participent activement à la supervision de la gestion de la sécurité informatique.
6. Les dirigeants de mon entreprise considèrent la sécurité comme un avantage concurrentiel.
7. Le responsable de la sécurité informatique de mon entreprise dispose d'une expertise et de moyens suffisants pour mettre en place un dispositif de sécurité solide.
8. Mon entreprise réalise des investissements pertinents dans des outils de sécurité de pointe tels que l'apprentissage automatique, l'automatisation, la robotisation, l'analyse et/ou l'intelligence artificielle.
9. Mon entreprise participe activement au partage d'information des cyber-menaces avec d'autres entreprises et le gouvernement.
10. Mon entreprise consacre des ressources importantes à l'évaluation des risques liés à la sécurité des tiers (y compris le *cloud* et l'ensemble de la chaîne de production).
11. Mon entreprise consacre des ressources importantes au recrutement et à la fidélisation du personnel chargé de la sécurité informatique.
12. Mon entreprise consacre des ressources importantes à la sensibilisation des employés aux règles de sécurité.
13. Les techniques de sécurité de mon entreprise sont suffisantes pour protéger les données et l'infrastructure informatique.
14. Mon entreprise est bien préparée à faire face aux violations de données et aux attaques de cybersécurité.
15. Les objectifs de sécurité informatique de mon entreprise sont alignés sur les objectifs commerciaux.
16. La direction de la sécurité informatique de mon entreprise prend en charge la sécurité dans un environnement DevOps.
17. La direction de sécurité informatique de mon entreprise prend en charge la sécurité dans un environnement DR et BCM.
18. La direction de la sécurité informatique de mon entreprise respecte les exigences en matière de protection des données et de la vie privée.
19. La direction de la sécurité informatique de mon entreprise est capable de prévenir la plupart des cyberattaques.
20. La direction de la sécurité informatique de mon entreprise est capable de détecter la plupart des cyberattaques.
21. La direction de la sécurité informatique de mon entreprise est capable de contenir la plupart des cyberattaques.
22. La direction de la sécurité informatique de mon entreprise est capable de détecter les attaques de type *zero-day*.
23. L'architecture de la sécurité informatique de mon entreprise présente un haut niveau d'interopérabilité (capacité de matériels, de logiciels ou de protocoles différents à fonctionner ensemble et à partager des informations), de flexibilité et de rapidité d'exécution.
24. La direction de la sécurité informatique de mon entreprise s'empresse de tester et d'installer tous les correctifs de sécurité.
25. La direction de la sécurité informatique de mon entreprise effectue des évaluations et/ou des audits pour identifier les menaces, les vulnérabilités et les attaques.
26. La direction de la sécurité informatique de mon entreprise effectue des évaluations et/ou des audits pour déterminer la conformité aux politiques de sécurité, aux procédures opérationnelles standard et aux exigences externes.
27. La direction de la sécurité informatique de mon entreprise applique rigoureusement les actes de non-conformité aux politiques de sécurité, aux procédures d'exploitation standard et aux exigences externes.
28. La direction de la sécurité informatique de mon entreprise est impliquée dans la détermination de l'utilisation adéquate des technologies perturbatrices (appareils mobiles, le *cloud*, les réseaux sociaux, les appareils IoT - *Internet of Things*) sur le lieu de travail.
29. La direction de la sécurité informatique de mon entreprise a la capacité de connaître l'emplacement physique des données sensibles.
30. La direction de la sécurité informatique de mon entreprise a la capacité de déclencher des mesures de lutte contre les attaques afin d'obtenir des informations sur l'attaquant.
31. La direction de la sécurité informatique de mon entreprise a évolué au fil du temps en raison de l'évolution des attaques et des types d'attaques.

Indice de cyber-menace

Un questionnaire composé de 10 questions a été élaboré. Celles-ci sont utilisées afin de représenter les expériences réelles des entreprises au cours des 12 derniers mois. Les réponses sont mesurées à l'aide des critères suivants :

TABLE 1.4 – Notation des questions de cyber-menace

Questions 1 - 3	Questions 4 - 6 et 8 - 9	Questions 7 et 10	Note (/10)
Nombre d'incidents	Probabilité de survenance	Risque	
Aucun	Aucune	Très faible	0
1 - 2	Peu probable	Faible	2,5
3 - 6	Assez probable	Modéré	5
7 - 10	Probable	Élevé	7,5
> 10	Très probable	Très élevé	10

Afin de déterminer l'indice de cyber-menace, l'institut Ponemon décida de faire une moyenne arithmétique sur l'ensemble des notes en considérant le poids de chaque réponse comme identique.

FIGURE 1.13 – Indice de cyber-menace

TABLE 1.5 – Questionnaire sur la cyber-menace

Questions
1. Combien d'incidents distincts de violation de données impliquant la perte ou le vol d'enregistrements de clients votre organisation a-t-elle connu au cours des 12 derniers mois ?
2. Combien d'incidents distincts de violation de données impliquant la fuite de systèmes d'information votre organisation a-t-elle connu au cours des 12 derniers mois ?
3. Combien de cyber-attaques distinctes ayant infiltré les réseaux et/ou les systèmes informatiques votre entreprise a-t-elle subi au cours des 12 derniers mois ?
4. Quelle est la probabilité que votre entreprise soit confrontée à une violation des données de ses clients dans les 12 prochains mois ?
5. Quelle est la probabilité que votre entreprise soit confrontée à une violation de données impliquant la fuite d'informations au cours des 12 prochains mois ?
6. Quelle est la probabilité que votre entreprise subisse une ou plusieurs cyber-attaques infiltrant vos réseaux ou systèmes informatiques au cours des 12 prochains mois ?
7. Évaluer chaque type de données à l'aide de l'échelle de risque présent dans le tableau précédent : informations confidentielles entre avocat et client, informations confidentielles de l'entreprise, données sur les consommateurs, comptes clients, informations financières, informations sur la R&D, ...
8. Évaluer chaque menace à l'aide de l'échelle de probabilité présent dans le tableau précédent : attaque par rançongiciel, attaque par déni de service, attaque par hameçonnage, attaque par point d'eau, ...
9. Évaluer chaque conséquence négative qu'une cyber-attaque peut provoquer à votre entreprise à l'aide de l'échelle de probabilité présent dans le tableau précédent : perte de revenus, perte de propriété intellectuelle, matériel volé ou endommagé, baisse de productivité, atteinte à la réputation, ...
10. Évaluer chaque points présentant des risques de sécurité dans votre infrastructure informatique aujourd'hui avec l'échelle de risque présent dans le tableau précédent : environnement des serveurs DNS, systèmes d'exploitation, applications tierces, ordinateurs, pénurie de personnel qualifié, ...

Construction d'un nouvel indicateur de risque

Dans le cadre de nos travaux, très peu de données (voire aucune donnée) concernant l'exposition des entreprises sont disponibles. En effet, le cas idéal aurait été de disposer d'une base de données composé des variables suivantes :

- Taille de l'entreprise : TPE, PME, ETI, ... ;
- Secteur d'activité : Finance, commerce, ... ;
- Existence d'un RSSI (Responsable de la Sécurité des Systèmes d'Information) : Oui, Non ;
- Niveau de formation des personnels : Note entre 0/3 et 3/3 ;
- Nombre d'attaques ;
- Date des attaques ;
- ...

Afin de palier ce problème nous allons essayer de construire un indice de risque avec comme seule entrée le nombre de sinistres reporté selon une date donnée. L'indice de risque doit varier de la façon suivante : lorsque l'indice de risque augmente, le nombre d'attaques réussie doit également augmenter. En effet, cet indice est semblable à un indice de menace ou encore de « vulnérabilité » que les entreprises ont face aux évènements cyber. A l'inverse, plus l'indice de risque diminue, moins les entreprises auront tendances à se faire attaquer. Cependant, il faudra prendre en compte un temps de décalage entre la dynamique de cet indice et la dynamique des sinistres. Si l'indice de risque augmente à un instant t, le nombre d'attaques ne va pas augmenter à l'instant t mais augmentera à un instant $t + \delta$ ($\delta > 0$). Afin de pouvoir modéliser tous ces éléments, nous nous sommes donc orientés vers le modèle de Lotka-Volterra que nous étudierons par la suite. Avec ce dernier, il serait possible d'établir un lien direct entre cet indice et le niveau de sinistralité.

Chapitre 2

Modélisation théorique de Lotka-Volterra

Ce chapitre a pour objectif la modélisation du modèle proie-prédateur à l'aide d'une base de données publique sur l'assurance violations de données. Pour ce faire, une étude sur le nombre de cyber-attaques réussies a été réalisée.

Dans la *première partie*, la base de données PRC qui a été utilisée lors de l'étude sera présentée.

Puis, dans une *seconde partie*, une présentation de l'intérêt d'une modélisation du modèle de Lotka-Volterra sur le nombre de violations de données ainsi que le formalisme mathématique associé seront développés.

Quant à l'analyse et l'interprétation des résultats obtenus lors de la modélisation, ils seront étudiés dans une *troisième partie*. Cette dernière permettra de comprendre les tendances obtenus lors de la modélisation. Nous présenterons également les limites de la modélisation actuelle de par le fort biais que présente la base de données mais également du fait de la complexité du risque cyber.

2.1 Présentation des données publiques

Afin de modéliser le modèle de Lotka-Volterra, nous allons utiliser la base de données PRC. Celle-ci a été développée par une association de sensibilisation aux risques liés à la vie privée basée aux États-Unis. Elle est l'une des seules qui ressemble de plus près à une base de données classique en assurance. En effet, elle associe une « fréquence » à une sévérité. Plusieurs travaux actuariels ont été menés avec cette base de données comme ceux présentés par Eling et al [9]. L'organisation *Privacy Rights Clearinghouse* répertorie les violations de données de 2005 à 2019 aux États-Unis. Elle est constituée des variables suivantes :

TABLE 2.1 – Description base de données PRC

Variables	Descriptions	Ordres de grandeur
Date made public	Date de déclaration du sinistre	3331 dates de déclaration
Company	Nom de l'entreprise sinistré	7669 entreprises
City	Ville où se situe l'entreprise	1550 villes
State	État où se situe l'entreprise	117 états
Type of breach	Type d'attaque	8 types d'attaques
Type of organization	Secteur d'activité de l'entreprise	8 types d'entreprises
Total records	Nombre de données volées	9015 entrées
Description of incident	Description du sinistre	×
Information source	Source d'information	18 sources d'informations
Year of breach	Année du sinistre	2015 à 2019
Latitude	×	×
Longitude	×	×

Zoom sur la variable Type of breach

Dans le graphique ci-dessous, il est observé que la base de données est composée principalement de piratage à l'aide de logiciel malveillant représentant 28% des attaques totales. De plus, les sinistres liés à la divulgation non intentionnelle ainsi que les sinistres liés à la perte ou le vol de documents papiers représentent respectivement 21% et 19%. Ces trois types d'attaques représentent à eux seuls 68% de la sinistralité totale.

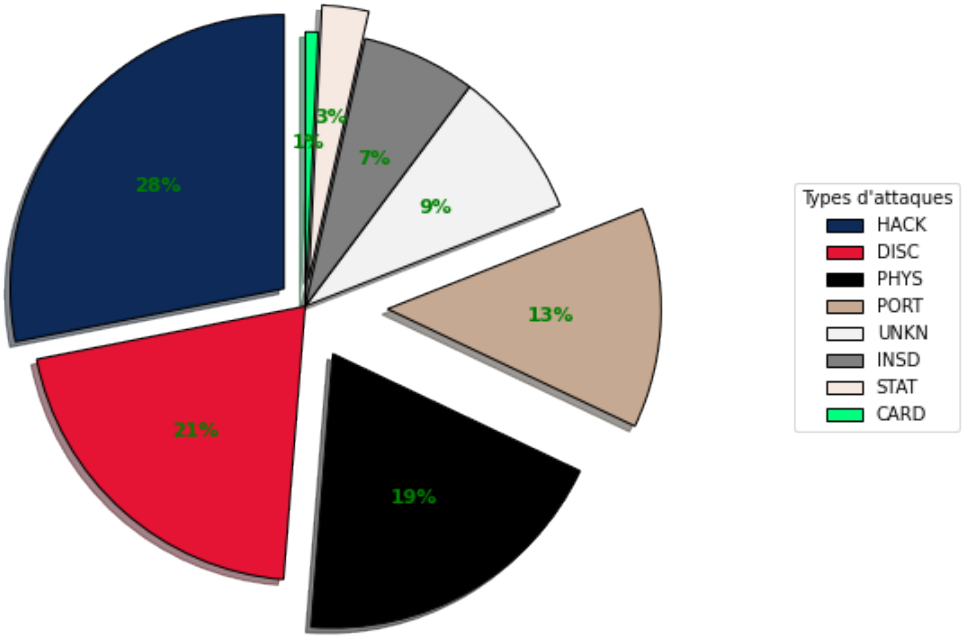

FIGURE 2.1 – Répartition des types d'attaques

TABLE 2.2 – Description variable *Type of breach*

Valeurs	Descriptions
HACK	Piratage à l'aide de logiciels malveillants
PORT	Equipements électroniques (clé usb, téléphone, ...) perdus, volés ou piratés
STAT	Ordinateur fixe perdu, volé ou piraté
INSD	Personne de l'entreprise enfreignant les données intentionnellement
DISC	Divulgation non intentionnelle (mauvais destinataire, ...)
UNKN	Type d'attaque non déterminé
PHYS	Documents papiers perdus/volés
CARD	Fraude à la carte bancaire

Zoom sur la variable Type of organization

Le graphique ci-dessous représente la répartition des secteurs d'entreprises sinistrés. La base de données est constituée de 48% d'organismes de santé. Ce phénomène pourrait être lié à l'importance des données du secteur médical. Ces données comprennent les informations relatives à une personne physique (nombre de pas, apports caloriques, ...), les informations obtenues lors d'un examen clinique (prise de sang, radiologie, ...), ainsi que les informations liées à une maladie (prestations de soins, traitements, ...). De plus, ces données sont de natures pérennes comparé aux données des services financiers.

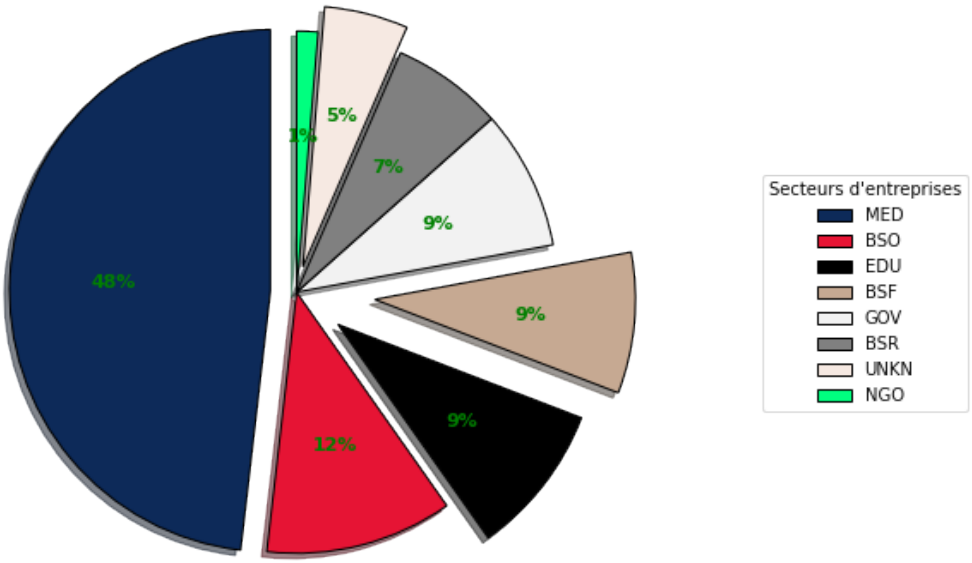

FIGURE 2.2 – Répartition des secteurs d'entreprises

TABLE 2.3 – Description variable *Type of organization*

Valeurs	Descriptions
EDU	Établissements d'enseignement
BSO	Autres types d'entreprises
MED	Organismes de santé
BSF	Entreprises, services financiers et assurances
BSR	Commerces
GOV	Gouvernement et armée
NGO	Organismes à but non lucratif
UNKN	Type d'entreprise non déterminé

La répartition des attaques selon le secteur d'entreprise présentée ci-dessous est très hétéroclite. En effet, nous observons que certains secteurs comme le secteur médical possèdent une très forte « fréquence » de sinistralité de l'ordre de plusieurs centaines de sinistres par an. A l'inverse, les gouvernements ainsi que les armées répertorient au maximum 20 attaques sur l'année 2012.

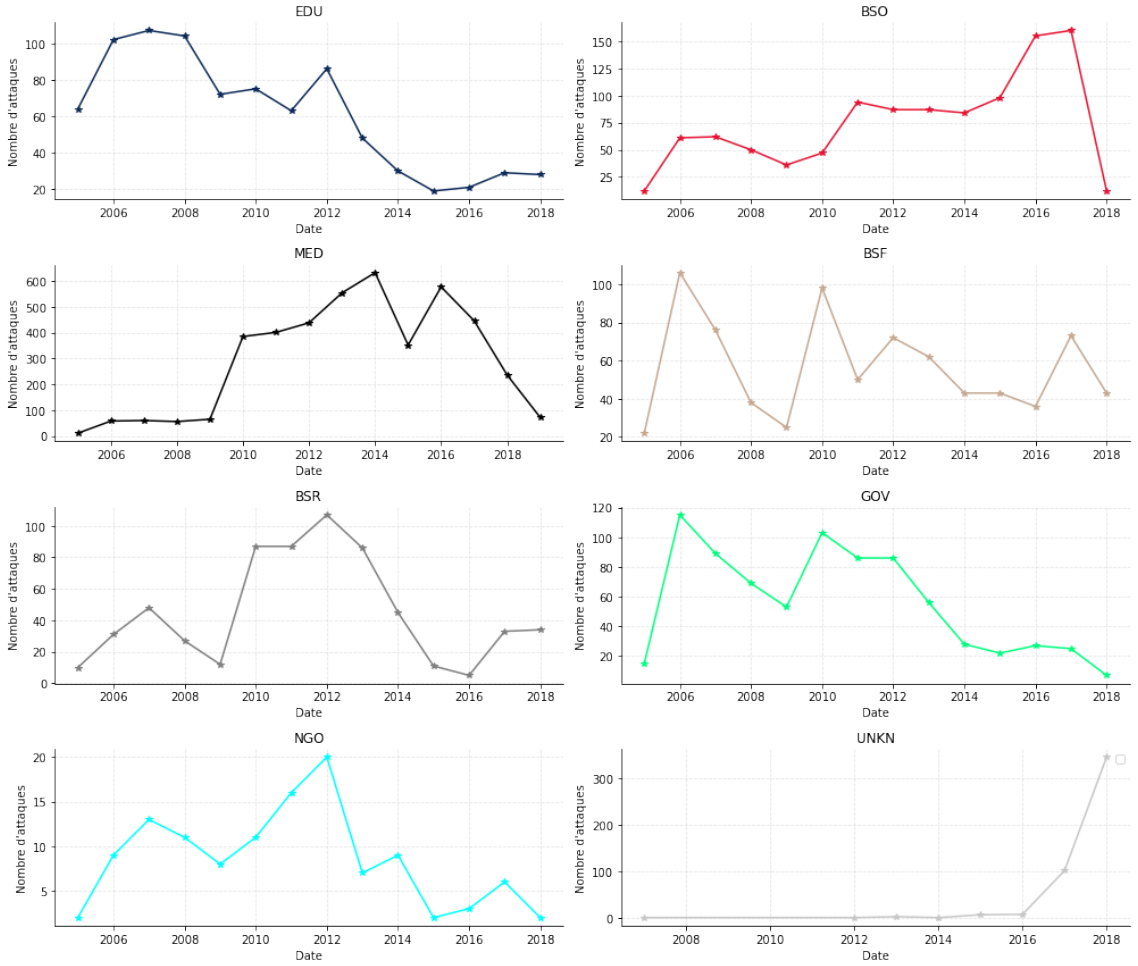

FIGURE 2.3 – Évolution du nombre d'attaques selon les secteurs d'entreprises

Les différences observées ci-dessus peuvent s'expliquer d'une part par la typologie des données évoquée précédemment. Mais également du fait que certains organismes sont plus ou moins « exposés » face au risque cyber. La quantification de la menace cyber sera étudiée dans la deuxième partie du chapitre.

Après constatation du lien entre nombre de sinistres et indice de risque cyber, plusieurs motivations ont dirigé cette étude vers la modélisation du modèle proie-prédateur :

- La première est le lien étroit qui existe entre l'attaque et la faute. Une cyber-attaque résulte d'une faute intentionnelle ou non intentionnelle. De ce fait, il existe une très forte corrélation entre ces phénomènes. Le modèle présenté ci-dessous par Lotka-Volterra permettra de modéliser à l'aide de deux populations : les proies (l'indice de risque cyber des entreprises) et les prédateurs (les cyber évènements) ;

- Le phénomène que nous observons est temporel et incertain. Notre objectif est de reconstruire cette dynamique et de déterminer à partir de cette dernière un indice de risque qui, à terme, découlera sur une tarification de police cyber.

2.2 Modélisation

2.2.1 Présentation du modèle

Peu après la première guerre mondiale, le mathématicien Vito Volterra consulta un biologiste (U. D'Ancona) qui analysa le phénomène suivant. En étudiant les résultats des pêches de certains ports (notamment celui de Venise), ce spécialiste avait estimé la proportion de requins pêchés parmi les poissons consommables et ce par rapport à la population totale des poissons de la mer Adriatique. Durant la première guerre mondiale, D'Ancona avait constaté que l'arrêt de la pêche a eu pour conséquence, non pas une augmentation équivalente des deux populations mais seulement une augmentation des requins. Cette tendance s'inversa avec la reprise de la pêche dès la fin de la guerre.

Volterra repris le problème de D'Ancona et mis au point un modèle qui fut au départ très simpliste. Dans un premier temps, il divisa les populations en deux groupes : les poissons qui se nourrissent d'autres poissons (prédateurs) et les poissons qui sont mangés par les prédateurs (les proies). Il supposa afin de faciliter sa méthode que le nombre de proie et de prédateur est très grand. De ce fait, il était possible de décrire l'évolution des proies $(y_1(t))$ et des prédateurs $(y_2(t))$ par un système d'équation différentielle. Lotka a proposé en même temps et de façon indépendante le même modèle. C'est pourquoi, nous parlons du modèle de Lotka-Volterra ou modèle proie-prédateur. Ce modèle se présente de la façon suivante : pour tout temps t,

$$\begin{cases} \frac{dy_1(t)}{dt} = y_1(t)\big(a - by_2(t)\big); \\ \frac{dy_2(t)}{dt} = y_2(t)\big(-c + dy_1(t)\big). \end{cases} \quad \text{avec } y_1(t_0) = y_1(0),\ y_2(t_0) = y_2(0). \tag{L-V}$$

TABLE 2.4 – Description des variables du modèle Lotka-Volterra

Variable	Description
t	Temps
$y_1(t)$	Nombre de proies en fonction du temps
$y_2(t)$	Nombre de prédateurs en fonction du temps
$\frac{dy_1(t)}{dt}$	Variation des proies au cours du temps
$\frac{dy_2(t)}{dt}$	Variation des prédateurs au cours du temps
$a > 0$	Taux de reproduction des proies
$b > 0$	Taux de mortalité des proies dû aux prédateurs
$c > 0$	Taux de mortalité des prédateurs
$d > 0$	Taux de reproduction des prédateurs

Dans le cadre de l'étude et de l'application au risque cyber, nous voudrions exprimer les dynamiques suivantes : l'indice de risque est supposé croître dans le temps tant que les entreprises ne se rendent pas compte du niveau de menace cyber qu'elles encourent $(ay_1(t))$. Cependant, lorsque les entreprises ont repéré leur niveau de risque, elles vont essayer de le baisser au maximum en formant ses employés ou encore en mettant à jour les logiciels $(-by_1(t)y_2(t))$. Le nombre de sinistres, quant à lui, diminue au fil du temps à cause des

mesures qui sont mises en place à la fois par la législation mais également par les entreprises en général ($-cy_2(t)$). Néanmoins, lorsque les entreprises agissent sur l'indice d'exposition en utilisant des mesures de sécurité afin de baisser ce dernier, elles auront tendance à ne plus faire attention aux attaques pouvant survenir à l'avenir. Ce phénomène engendrera donc une hausse de sinistralité ($dy_1(t)y_2(t)$) qui pourrait être expliquée par une potentielle nouvelle faille. En effet, si une entreprise a un indice de risque très faible, elle aura tendance à se relâcher au niveau de sa sécurité informatique. Ceci engendrera donc une hausse de l'indice de risque qui impactera à son tour le niveau de sinistralité.

En résumé, les variables du modèle retranscrivent les éléments suivants (dans le cadre de l'assurance cyber) :

TABLE 2.5 – Description variable du modèle Lotka-Volterra

Variable	Description
t	Mois
$y_1(t)$	Indice de risque cyber
$y_2(t)$	Nombre d'attaques réussies / Nombre de sinistres
$\frac{dy_1(t)}{dt}$	Variation de l'indice de risque cyber au cours du temps
$\frac{dy_2(t)}{dt}$	Variation du nombre de sinistres au cours du temps
$a > 0$	Taux de croissance de l'indice de risque
$b > 0$	Facteur de déclin de l'indice de risque
$c > 0$	Facteur de déclin du nombre de sinistres
$d > 0$	Taux de croissance du nombre de sinistres

Il faut noter que l'existence et l'unicité sont assurés via le théorème de Cauchy-Lipschitz.

Théorème 1 (Positivité des solutions)**.** *Soient $y_{1,0}$, $y_{2,0}$ des réels strictement positifs et t_0 un réel quelconque. Alors, la solution du problème de Cauchy*

$$\begin{cases} \left(\frac{dy_1(t)}{dt}, \frac{dy_2(t)}{dt}\right) = F\big(t, y_1(t), y_2(t)\big); \\ \big(y_1(t_0), y_2(t_0)\big) = (y_{1,0}, y_{2,0}). \end{cases}$$

vérifie pour tout réel t

$$\begin{cases} y_1(t) > 0; \\ y_2(t) > 0. \end{cases}$$

Théorème 2 (Périodicité des solutions)**.** *Toute solution du système de Lotka-Volterra est périodique.*

2.2.2 Résolution numérique

Les équations de Lotka-Volterra ne peuvent pas se résoudre analytiquement. Afin de déterminer une solution, il faudra s'intéresser à la discrétisation et à la résolution numérique. Pour ce faire, deux méthodes numériques seront choisies :

- La méthode d'Euler ;
- La méthode de Runger-Kutta d'ordre 4.

Durant la modélisation des deux méthodes, l'étude considérera un système d'équation différentielle ordinaire (EDO) sous la forme suivante :

$$Y'(t) = F(t, Y(t)), \qquad t \in [t_0, t_f], \tag{Syst}$$

où $Y(t) = (y_1(t), y_2(t))^T$ et $F(t, Y(t)) = (f_1(t, Y(t)), f_2(t, Y(t)))^T$, avec $Y(t_0) = (y_{1,0}, y_{2,0})^T$.

Méthode d'Euler

La méthode d'Euler, du mathématicien Léonhard Euler (1707 - 1783), est une procédure numérique permettant de résoudre par approximation des équations différentielles du premier ordre avec une condition initiale. Cette méthode est la plus simple des méthodes de résolution numérique des équations différentielles.

Le schéma d'Euler associé à ce système permet de résoudre cette EDO et s'écrit de la façon suivante :

$$\begin{cases} t_{n+1} = t_n + h_n; \\ y_{1,n+1} = y_{1,n} + h_n f_1(t_n, y_{1,n}, y_{2,n}); \qquad t \in [t_0, t_f]. \\ y_{2,n+1} = y_{2,n} + h_n f_2(t_n, y_{1,n}, y_{2,n}). \end{cases} \tag{Schéma-Euler}$$

Méthode de Runge-Kutta d'ordre 4

La méthode de Runge-Kutta, des mathématiciens Carl Runge et Martin Wilhelm Kutta (1901), repose sur le principe de l'itération. En effet, une première estimation de la solution est utilisée afin de calculer une seconde estimation qui sera plus précise et à son tour utilisée pour calculer une troisième estimation etc.

Le schéma de la méthode de Runge-Kutta s'écrit de la façon suivante :

$$\begin{cases} p_{1,1} = f_1(t_n, y_{1,n}, y_{2,n}); \\ p_{1,2} = f_2(t_n, y_{1,n}, y_{2,n}); \\ p_{2,1} = f_1\left(t_n + \frac{h_n}{2}, y_{1,n} + \frac{h_n}{2} p_{1,1}, y_{2,n} + \frac{h_n}{2} p_{1,2}\right); \\ p_{2,2} = f_2\left(t_n + \frac{h_n}{2}, y_{1,n} + \frac{h_n}{2} p_{1,1}, y_{2,n} + \frac{h_n}{2} p_{1,2}\right); \\ p_{3,1} = f_1\left(t_n + \frac{h_n}{2}, y_{1,n} + \frac{h_n}{2} p_{2,1}, y_{2,n} + \frac{h_n}{2} p_{2,2}\right); \\ p_{3,2} = f_2\left(t_n + \frac{h_n}{2}, y_{1,n} + \frac{h_n}{2} p_{2,1}, y_{2,n} + \frac{h_n}{2} p_{2,2}\right); \\ p_{4,1} = f_1(t_n + h_n, y_{1,n} + h_n p_{3,1}, y_{2,n} + h_n p_{3,2}); \\ p_{4,2} = f_2(t_n + h_n, y_{1,n} + h_n p_{3,1}, y_{2,n} + h_n p_{3,2}); \\ y_{1,n+1} = y_{1,n} + \frac{h_n}{6}\left(p_{1,1} + 2p_{2,1} + 2p_{3,1} + p_{4,1}\right); \\ y_{2,n+1} = y_{2,n} + \frac{h_n}{6}\left(p_{1,2} + 2p_{2,2} + 2p_{3,2} + p_{4,2}\right). \end{cases} \tag{Système-Runge-Kutta}$$

2.2.3 Comparaison des deux méthodes de résolution

Afin de comparer les deux méthodes de résolution, deux graphiques seront présentés. Le premier présente la dynamique des proies et des prédateurs au fil du temps. Quant au

second, il représente le caractère périodique des solutions en représentant les prédateurs en fonction des proies. Ci-dessous, un schéma explicatif est présenté permettant d'aider l'analyse et la compréhension des graphiques qui seront rencontrés dans la suite du mémoire.

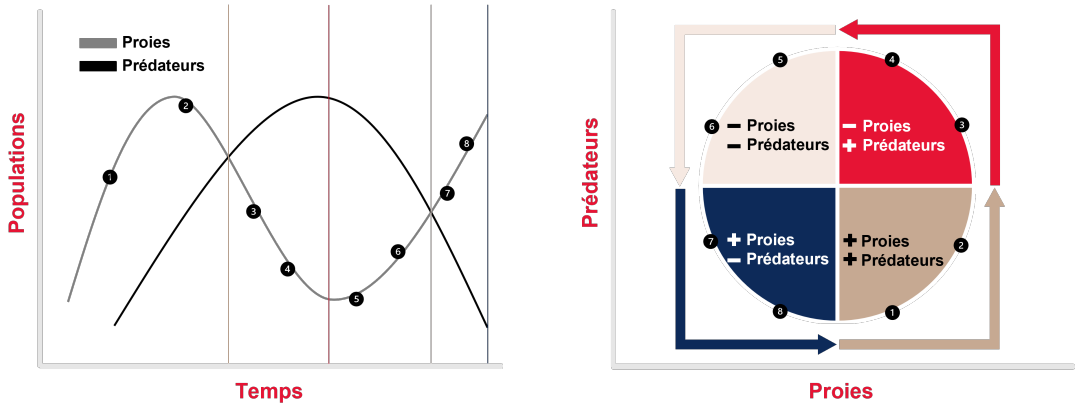

FIGURE 2.4 – Schéma explicatif de la dynamique des populations

Dans un premier temps, l'implémentation de la méthode d'Euler a été opérée. Ce modèle a permis de comparer l'évolution des populations. Pour cela, il a fallu prendre des paramètres comme exogènes en respectant l'hypothèse que $a, b, c, d > 0$.

En posant $a = 2, b = c = d = 1$, une pseudo-périodicité est observée entre l'évolution de la population des proies et des prédateurs à l'aide du graphique de gauche. Certaines irrégularités sont également observées dans les oscillations qui peuvent être représentées par un portrait de phase (courbe utilisée pour l'étude des systèmes dynamiques représentant y en abscisse et x en ordonnée). En effet, à l'aide du graphique de droite, la courbe se présente sous forme de spirale et non comme une ellipse. De ce fait, si nous avions pris une période de temps plus longue, nous aurions eu une troisième spirale prouvant qu'il existe un attracteur en 0. En testant des valeurs de paramètres différentes, il advient que le modèle est très sensible à la valeur des coefficients. C'est pourquoi la méthode d'Euler présentait certaines limites comme le fait qu'elle soit très coûteuse. Afin de palier cela, il est néanmoins possible d'augmenter le nombre d'itération ou bien de réduire le pas utilisé.

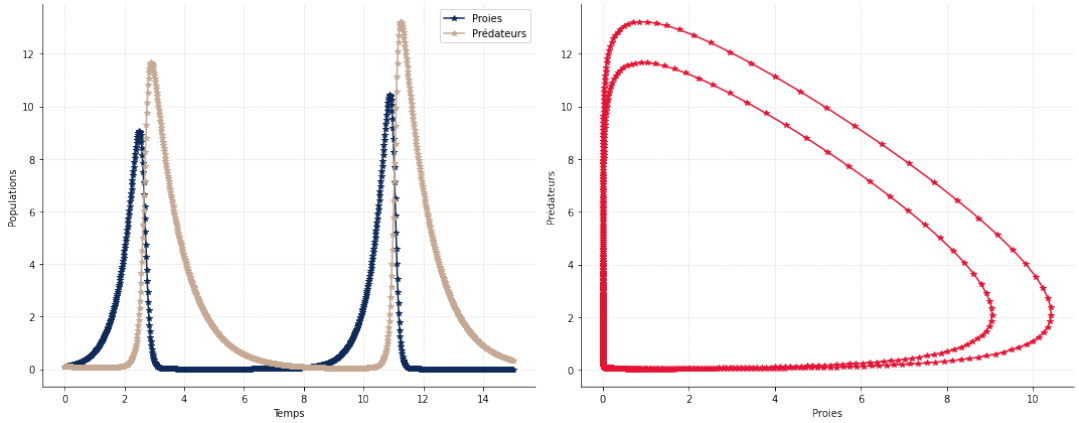

FIGURE 2.5 – Évolution de la population des proies et prédateurs avec la méthode d'Euler

Mais, l'implémentation d'une meilleure méthode de résolution numérique des EDO a été privilégiée : la méthode de Runge-Kutta d'ordre 4. Cette méthode, contrairement à celle d'Euler, montre la périodicité de l'évolution des proies et des prédateurs. Pour appuyer ces propos, il est possible d'observer le portrait de phase sur le graphique de droite. Ce dernier est représenté non plus par une spirale mais par une ellipse : il n'existe donc aucun point d'attraction ou de répulsion. Le système est donc stable dans le temps. C'est pourquoi, grâce à ce résultat, il est possible de voir la puissance de la méthode de Runge-Kutta d'ordre 4 et, a contrario, la faiblesse du schéma d'Euler.

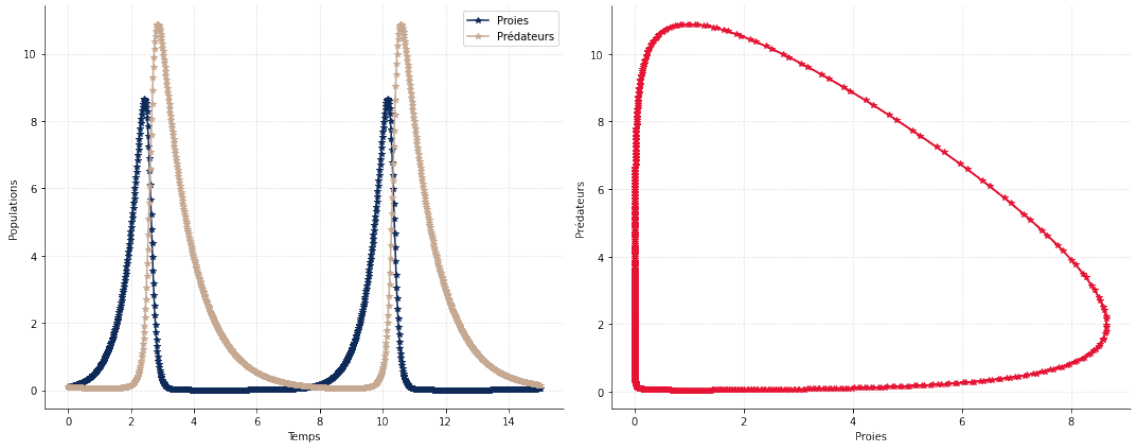

FIGURE 2.6 – Évolution de la population des proies et des prédateurs avec la méthode de Runge-Kutta d'ordre 4

2.2.4 Limites du modèle

Le modèle de base repose sur des hypothèses fortes :

- La nutrition des prédateurs ne dépend que de la taille de la population des proies. Dans la situation de l'étude, cela consisterait à dire que le nombre de sinistres est dû simplement à l'indice de risque des entreprises et à aucun autre élément ;
- Les prédateurs ont un appétit illimité et n'entrent jamais en compétition entre eux. Ici, il est supposé que tous les cyber-criminels travaillent ensemble et ne rentrent jamais en conflit ;
- L'environnement ne change pas « en faveur » d'une espèce et l'adaptation est trop lente pour être perceptible dans le modèle. Afin d'appliquer le modèle de Lotka-Volterra, il a fallu préalablement supposer que les entreprises ne pouvaient pas réagir face aux cyber-attaques ;
- Même si l'une des populations est réduite à un très petit effectif, elle pourra toujours se régénérer : cette hypothèse considère donc qu'il n'y aura jamais d'extinction.

2.2.5 Application à la base de données

Afin d'appliquer le modèle de Lotka-Volterra, l'étude reprendra la base de données PRC. Le but sera de modéliser le nombre d'attaques cyber (correspondant aux prédateurs) ainsi que l'indice de risque (correspondant aux proies). Pour ce faire, une segmentation a été

retenue aux niveaux des organisations. Dans un premier temps, les équations de Lotka-Volterra seront modélisées pour les commerçants mais le même schéma pourra être réitéré sur les autres organisations.

Dans le graphique ci-dessous, une représentation de l'évolution du nombre d'attaques a été effectuée pour les commerces. Un pic d'attaque réalisé en 2012 a été constaté. En effet, 107 attaques ont été recensées cette année là contre une moyenne sur 14 ans d'environ 44 sinistres.

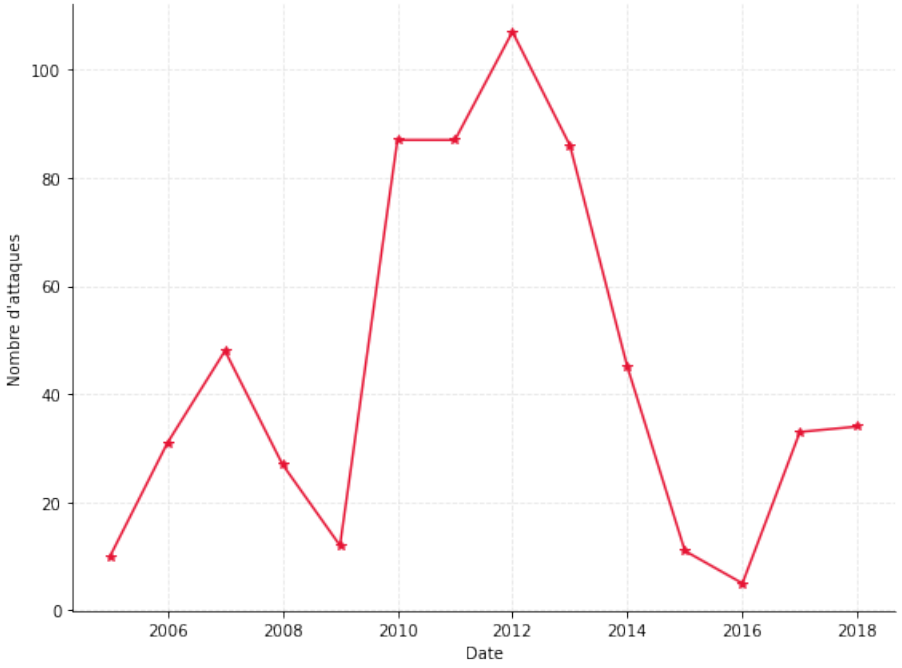

FIGURE 2.7 – Évolution du nombre d'attaques pour les commerces

La détermination du nombre de prédateurs est immédiate. En effet, la base de données recense la sévérité des attaques à l'aide de la variable *Total records*. Afin d'obtenir le nombre d'attaques annuellement, il suffit de compter les attaques recensées chaque ligne. Néanmoins, l'indice de risque n'est pas exprimée directement. C'est pourquoi, la première étape de la modélisation consista à déterminer la dynamique des prédateurs. Pour cela, les paramètres d'entrées $(a, b, c, d, y_{1,0}, y_{2,0})$ ont du être initialisés.

Le nombre de prédateurs $y_{2,0}$ a été initialisé selon le nombre d'attaques recensé en 2005. Quant aux autres paramètres, l'initialisation a été effectuée aléatoirement. En effet, le nombre de proies initial, c'est à dire $y_{1,0}$, a été supposé dans un premier temps égal à 45. Mais, ce nombre n'est qu'une supposition afin d'initialiser le modèle. Il est donc amené à évoluer durant la suite de la modélisation. Enfin, les paramètres de taux ont été initialisés arbitrairement tels que : $a = b = c = d = 0,01$. Notons que la condition de positivité des paramètres de taux a été respectée lors de l'initialisation.

Afin de déterminer les paramètres optimaux du modèle ainsi que le niveau de risque en 2005, la minimisation de la somme des écarts quadratiques entre la courbe générée par les paramètres d'entrées ainsi que la courbe représentant le nombre d'attaques a été effectuée. L'algorithme d'optimisation SLSQP (*Sequential Least SQuares Programming*) renvoie le résultat suivant :

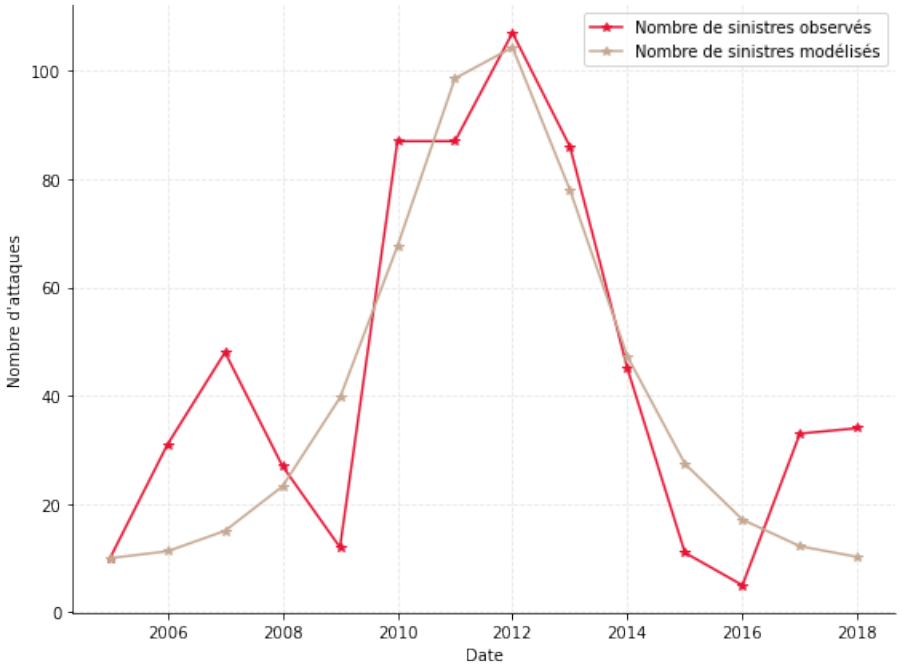

FIGURE 2.8 – Comparaison du modèle de Lotka-Volterra et du nombre d'attaques

Le résultat paraît dans un premier temps cohérent avec les données. En effet, la tendance de la courbe des prédateurs est semblable à celle des données. Cependant, le modèle ne tient pas compte des fluctuations. Le modèle a eu tendance à capter les grosses « fréquences » mais ne tiendrait pas compte des légères fluctuations du nombre d'attaques. Une fois les prédateurs déterminés, les proies sont déduites directement de ces dernières.

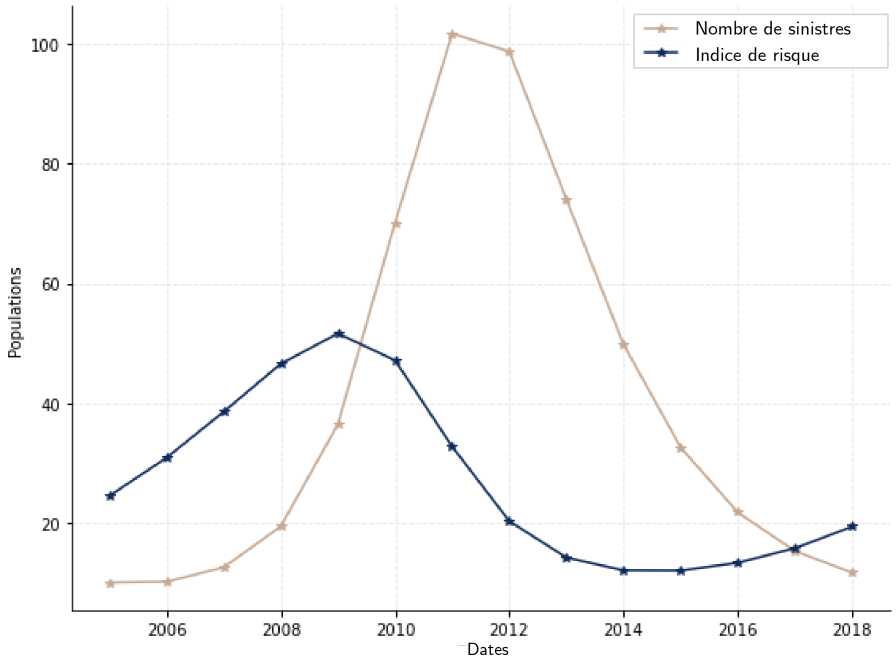

FIGURE 2.9 – Modèle de Lotka-Volterra

Ci-dessus, l'indice de risque est corrélé positivement à l'évolution du nombre de sinistres. En effet, à la première année observée, c'est à dire en 2005, l'indice de risque était plus fort que la sinistralité. Cet indice augmenta entre 2005 et 2009. Cette hausse engendra une hausse du niveau de sinistralité qui s'est opérée entre 2005 et 2011. Cependant, à partir de 2009, une baisse du niveau de risque a été constatée. Cette baisse permet d'anticiper une baisse de sinistralité future qui peut être due à un renforcement des entreprises sur les bonnes manières à adopter pour limiter les attaques cyber. Cette baisse d'indice de risque engendrera une baisse de sinistres avec un décalage temporel et ceux jusqu'à 2015. Un cercle vertueux se forme alors. En effet, à partir de 2015, l'indice de risque des entreprises croît, prédisant une hausse de sinistralité future ... Cependant, notons que la tendance globale du phénomène nous montre que le niveau de sinistralité et l'indice de risque des entreprises est stable au fil des années. C'est pourquoi, dans le chapitre suivant, nous modifierons les équations du modèle de base afin d'incorporer une possible tendance à la hausse ou à la baisse. Nous remarquons que les dynamiques de ces populations évoluent selon une périodicité semblable mais avec un décalage temporel. L'objectif de ce graphique est de montrer le lien fort entre indice de risque et nombre de sinistres afin de sensibiliser au mieux les entreprises à réagir le plus rapidement possible face aux vulnérabilités qu'elles ont identifiées.

2.3 Analyse et limites des résultats

Les résultats obtenus reposent sur des hypothèses trop fortes pour juger de l'intérêt du modèle sur ce jeu de données. En effet, la modélisation en cyber assurance est complexe de par :

- une volatilité très forte engendrant une variance « infinie » ;
- une grosse queue de distribution due à l'hétérogénéité de la population ;
- les assurés ne sont pas forcément indépendants ;
- le nombre d'assurés n est assez faible ;
- la rareté d'un événement ;
- en théorie, l'assuré dispose d'une information supérieure à l'assureur de son risque : asymétrie d'information. Mais ici, nous nous retrouvons dans le cas quasi-inverse car l'assuré n'est que peu renseigné sur son niveau de menace face aux risques cyber ;
- selon l'ANSSI, les personnes assurées ont tendance à être plus attaquées que les personnes non assurées ;
- l'aléa moral : le fait d'être assuré peut changer le comportement de l'assuré. Néanmoins, ce point n'est que peu observé dans l'assurance cyber ;
- une multitude de sinistres cyber ne sont pas déclarés : le *hunger for bonuses* correspond au fait de ne pas déclarer les sinistres à l'assureur car les coûts de réparations effectués par soi même sont inférieurs aux coûts de réparations effectués par l'assurance. En effet, les frais de l'assureur incluront le paiement d'une franchise ainsi que l'ajout d'un malus sur les primes des années suivantes ;
- l'estimation statistique est très problématique car les sources de données sont très biaisées.

Regardons de plus près le dernier point. Les sources de données proviennent principalement des organismes à but non lucratif, de la loi sur la portabilité et la responsabilité en matière d'assurance maladie, des États, ainsi que des médias. Cependant, nous observons une hétérogénéité des déclarations de sinistres. En effet, les organismes à but non lucratifs ont essentiellement remontés les cyber-attaques entre 2005 et 2015. Après 2015, la quasi-totalité des sinistres ne sont plus déclarés dans la base de données. À l'inverse, à partir de 2010, une hausse de déclaration des « gros » sinistres a vu le jour grâce à l'HIPAA qui est une série de normes réglementaires fédérales américaines qui décrivent l'utilisation et la divulgation légales des informations de santé protégées aux États-Unis. Cette réglementation impose la déclaration des sinistres à partir d'une forte sévérité. Quant aux états, une volonté de transparence naquit et, à partir de 2012, nous constatons une augmentation des déclarations. Enfin, concernant les médias, nous observons une hausse pérenne du niveau global des déclarations des sinistres cyber.

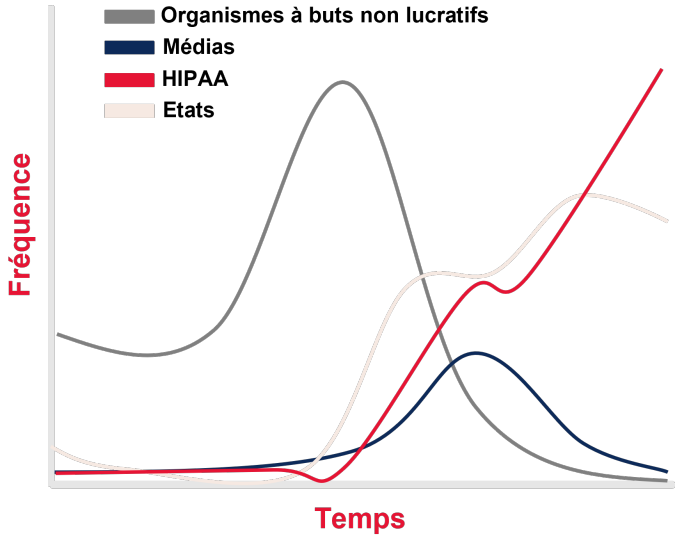

FIGURE 2.10 – Fréquence des sources d'informations

Nous constatons que certaines sources apparaissent au fil du temps alors que d'autres disparaissent. De ce fait, il est difficile de conclure sur la fréquence de sinistralité. En effet, une hausse du nombre d'attaques pourrait provenir d'une hausse des déclarations due aux contextes réglementaires qu'impose l'HIPAA mais également d'une hausse réelle de la sinistralité. Il en va de même pour les baisses de sinistralités observées. Il est très difficile d'affirmer avec certitude si une baisse est due à une prise de conscience des enjeux cyber par les organismes faisant baisser leur niveau réel de sinistralité ou simplement une baisse de déclaration due à l'extinction de la source des organismes à buts non lucratifs.

De plus, les problèmes liés au fait de collecter et de remonter les sinistres cyber à partir de différentes sources engendrent un nombre de sinistres non lisse. A l'aide de l'exemple des commerçants, ce phénomène est « assez peu » observé. Cependant, pour le reste des organisations, cela engendre de fortes fluctuations de sinistralités d'une année sur l'autre. Par conséquent, le modèle de Lotka-Volterra aura énormément de mal à s'adapter aux données.

Afin de palier ce problème, une base de données d'un assureur français sera utilisée par la suite. En effet, grâce à cette dernière, les données seront de meilleure qualité car nous

disposerons de plusieurs variables endogènes comme le coût du provisionnement ou encore la durée de restauration. Ces éléments seront connus de l'assureur. En revanche, le nombre de sinistres sera drastiquement plus faible car cette base recense environ 300 sinistres sur une fenêtre de temps de 2 ans et demi.

Chapitre 3

Application à un cas concret

Ce chapitre a pour objectif la modélisation du modèle proie-prédateur à l'aide d'une base de données française fournie par un assureur. Pour ce faire, une étude du nombre de cyber-attaques a été réalisée afin de construire l'indice de risque qui servira par la suite à tarifer les polices du portefeuille.

Dans la *première partie*, la base de données qui a été utilisée lors de l'étude sera présentée.

Puis, dans une *seconde partie*, la modélisation du modèle de Lotka-Volterra sur le nombre de sinistres sera présentée. Une transformation sera opérée au préalable en lissant la sinistralité à l'aide de la méthode de Whittaker-Henderson.

Quant à la tarification des polices d'assurance, elle sera étudiée dans une *troisième partie*. Cette dernière permettra d'établir dans un premier temps un tarif simple qui sera élaboré à l'aide d'une méthodologie semblable au régime des catastrophes naturelles.

La *quatrième partie*, consistera à reprendre les hypothèses utilisées dans le mémoire et à faire des tests de sensibilité sur ces dernières afin de regarder l'impact sur les primes ainsi que sur les S/P.

Enfin, la *dernière partie* consistera a discuter des limites de l'étude.

Attention : Durant la réalisation de l'étude, nous ne disposions que d'une population de sinistrés. C'est pourquoi, les S/P présentés ne sont pas réellement des ratios combinés car ils n'englobent que la prime des sinistrés et non celle de la population entière.

3.1 Présentation des données

Afin de pouvoir estimer aux mieux le nombre de sinistres et l'indice de risque des entreprises, il faut se fonder sur un historique de données non biaisé par les sources qui remontent les informations dans le but d'assurer une estimation plus robuste. Pour ce faire, nous utiliserons dans la suite de l'étude une base de données d'un assureur X. Cette dernière recense des cyber-attaques entre février 2019 et juillet 2021 de tout type contrairement à la base de données PRC. De plus, cette dernière inclut exclusivement des entreprises françaises. Ce dernier point permettra par la suite de comparer les résultats avec l'étude LUCY publiée par l'AMRAE. Cependant, nous ne nous attendons pas à obtenir les mêmes résultats que cette dernière.

Cette base de données est décomposée en trois blocs :

- Dans un premier temps les variables déterminent le référencement administratif des sinistres : date, police, CSP, ... ;
- Quant au second, il correspond au traitement du sinistre en comprenant une phase d'identification, de qualification/traitement puis une phase de restauration : durée de restauration, type d'attaques cyber, ... ;
- Enfin, un dernier bloc permet l'identification des coûts des sinistres et des éventuels recours : coût des dommages hors taxe, coût de gestion de la crise, coût provisionnel initial, ...

Zoom sur la variable Attaque

Dans le graphique ci-dessous, il est observé que la base de données est composée principalement de cryptovirus représentant 59% des attaques totales. De plus, les sinistres liés au *malware* représentent 14% de la sinistralité au globale. Ces deux types d'attaques décrivent à eux seuls 73% de la sinistralité totale soit environ les trois quarts de la sinistralité.

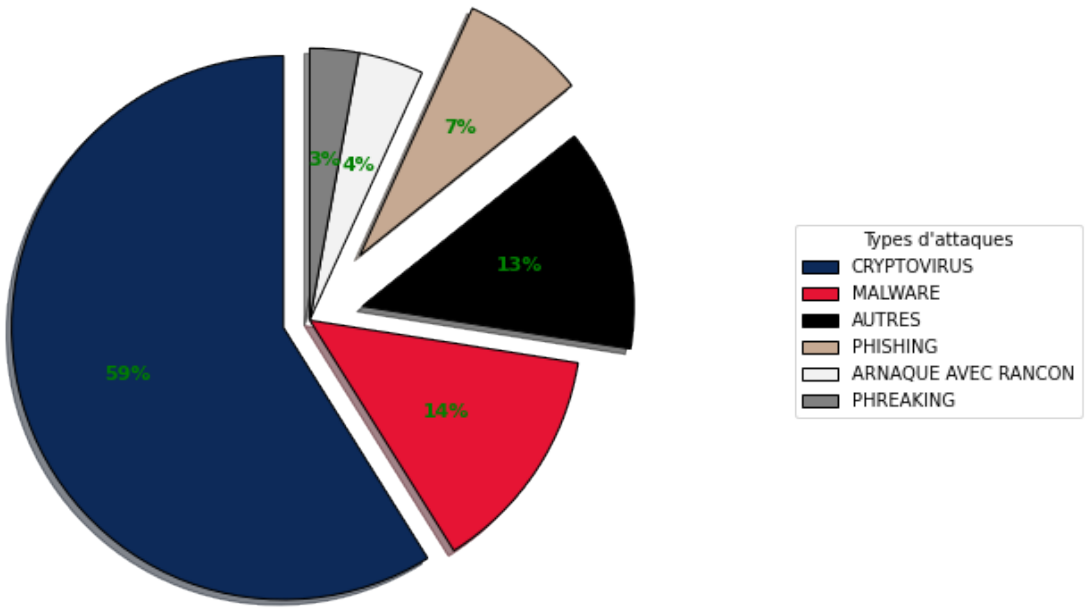

FIGURE 3.1 – Répartition des types d'attaques

TABLE 3.1 – Description variable Attaque

Valeurs	Descriptions
CRYPTOVIRUS	Programme informatique malveillant qui prend en otage les données en les chiffrant.
MALWARE	Logiciels malveillants comprennant des virus.
AUTRES	Tout autre type d'attaques (attaque par déni de service, défiguration, ...).
PHISHING	Attaque par hameçonnage.
ARNAQUE AVEC RANCON	Attaque par rançongiciel.
PHREAKING	Piratage téléphonique.

FIGURE 3.2 – Évolution des différentes attaques à travers le temps

Zoom sur la variable Metier

Le graphique ci-dessous représente la répartition des secteurs d'entreprises sinistrés. La base de données est constituée de 36% de professionnel. Les collectivités, les entreprises et les industries agricoles représentent quant à eux 53% de la sinistralité totale. A l'inverse, nous assistons à une sous représentation des associations ainsi que des métiers du bâtiments. En effet ils représentent respectivement 4% et 7% de la base de données. Contrairement aux entreprises qui disposent de données à caractères personnels, les métiers liés aux bâtiments ainsi que les associations sont possiblement moins concernés par le risque de vol de données sensibles. Cependant, cette représentation ne dit pas qu'un type d'organisation subit plus d'attaque qu'un autre. En effet, il faut rapporter ce pourcentage au nombre de personnes ayant souscrit un contrat d'assurance cyber.

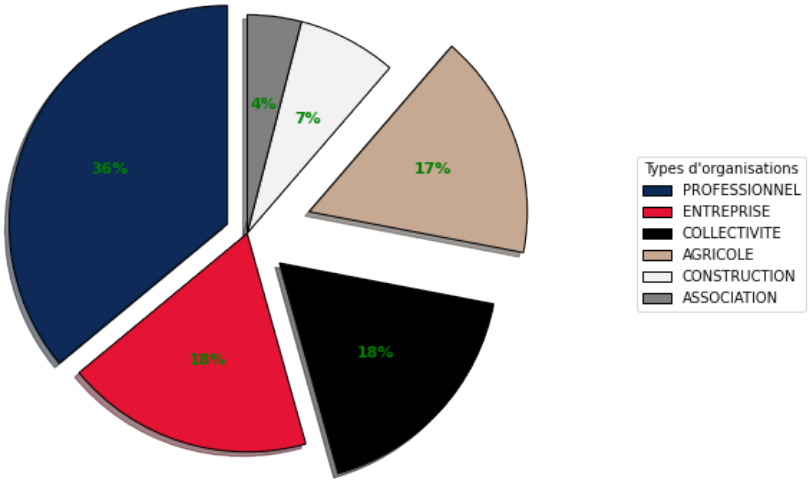

FIGURE 3.3 – Répartition des types d'organisations

Dans le graphique ci-dessous, une représentation de l'évolution du nombre d'attaques a été effectuée pour toutes les organisations confondues à un niveau mensuel. Un pic d'attaque réalisé en mai 2019 a été constaté. En effet, 24 attaques ont été recensées ce mois là contre une moyenne sur 31 mois d'environ 10 sinistres mensuels reportés. Il est possible de discerner trois ou quatre « cycles » d'attaques :

- 1er cycle : février 2019 - août 2019 ;
- 2ème cycle : août 2019 - août 2020 ;
- 3ème cycle : août 2020 - février 2021 (ou juillet 2021 en considérant 3 cycles) ;
- (4ème cycle : février 2021 - juillet 2021).

Notons également qu'au fur et à mesure des cycles, le nombre d'attaques ne cessent de diminuer (ou du moins le nombre de déclaration de sinistres).

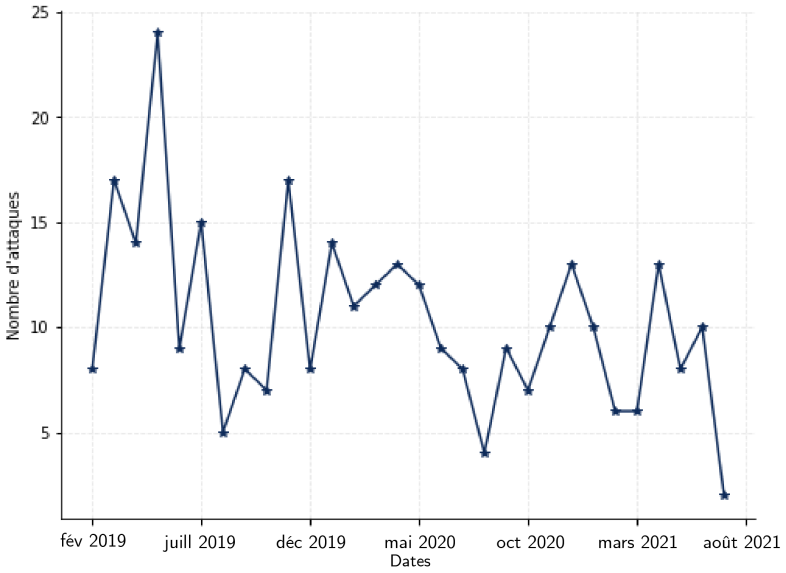

FIGURE 3.4 – Évolution du nombre d'attaques mensuel au global

Afin d'appliquer le modèle de Lotka-Volterra, il faudrait préalablement lisser nos données brutes. Le besoin de lissage est dû au caractère « accidenté » de la courbe. Deux hypothèses peuvent expliquer ce phénomène :

- Hypothèse 1 : la vraie courbe des sinistres est réellement « accidentée » (irrégulière) ;
- Hypothèse 2 : les erreurs d'estimation sont responsables (mauvaise qualité d'estimation due à une faible quantité de données).

La seconde hypothèse sera principalement choisie. En effet, le problème proviendrait principalement des fluctuations d'échantillonnage (problème de variance) que d'une vraie irrégularité structurelle des données.

Il existe plusieurs techniques de lissages (moyenne mobile, Whittaker-Henderson et bayésiens). Cependant, dans le cadre de l'étude, seul le lissage de Whittaker-Henderson sera abordé.

3.2 Modélisation

Lissage de Whittaker-Henderson

Ce modèle a été élaboré par E.T.Whittaker (1923) ainsi que R.Henderson (1924). Néanmoins, la méthode a drastiquement évoluée au fil du temps s'éloignant des propositions des auteurs. Dans le cadre du mémoire, cette méthode sera utilisée afin de lisser la sinistralité.

Nous allons chercher à estimer un vecteur q_x représentant la sinistralité au temps $x = 1, ..., m$. Cependant, nous disposons de la sinistralités brutes $\hat{q}_x$ comme estimateur préliminaire. A partir de la courbe des sinistres brutes, nous voudrions obtenir une meilleure estimation de la « vraie » courbe par une courbe « plus lisse » qui sera notée $q'_x(h)$ où h est un paramètre de lissage.

La méthode de Whittaker-Henderson permet de concilier deux objectifs contradictoires :

- Les $\hat{q}_x$ doivent être proche des q_x car ce sont des estimateurs non paramétriques (aucune hypothèse n'a été effectuée) : critère de fidélité ;
- Nous avons un a priori sur la courbe qui doit être lisse. Cependant, la courbe des sinistres brutes ne l'est pas : critère de régularité.

L'objectif de la modélisation sera de trouver le meilleur compromis entre le critère de fidélité et le critère de régularité.

Fidélité

Considérons une courbe quelconque notée c_x. En utilisant une distance quadratique (L^2) avec la courbe de sinistralité brute, nous obtenons :

$$F(c) = ||c - \hat{q}||^2_{2,w} = \sum_{x=1}^{m} w_x (c_x - \hat{q}_x)^2.$$

Régularité

Étant dans une version discrétisée, nous définissons l'opérateur différence :

$$\Delta : (c_x)_{x=1,\dots m} \longrightarrow (\Delta c_x)_{x=1,\dots,m-1},$$

où $\Delta c_x = c_{x+1} - c_x$.

Cet opérateur a la particularité de pouvoir être itéré :

$$\Delta^2 c = \Delta(\Delta c),\ \Delta^k c = \Delta(\Delta^{k-1} c).$$

Dire qu'une courbe est régulière revient à montrer que les dérivées (associées à cette dernière) d'un certain ordre sont « faibles ».

Le critère de régularité est alors définie comme :

$$S(c) = \sum_{x=1}^{m-z} (\Delta^z q_x)^2.$$

Le but du modèle est de minimiser $F(c)$ et $S(c)$. Cependant, lorsque $F(c)$ est minimal pour $\hat{q}$, $S(\hat{q})$ est très grand. C'est pourquoi, le critère de Whittaker-Henderson est définie comme

$$WH_h(c) = F(c) + hS(c).$$

L'objectif est alors de déterminer $q'_x(h) = \arg\min_c\ WH_h(c)$.

Deux cas limites sont à discuter :

- Lorsque $h \longrightarrow 0 : q'_x(h) \longrightarrow \hat{q}_x$. Dans ce cas, aucune importance n'est accordée au critère de régularité (aucun lissage n'est effectué) ;
- Lorsque $h \longrightarrow \infty : q'_x(h) \approx k$ où k est une constante.

Dès lors que le h qui minimise le critère WH a été déterminé, $q'_x(h)$ s'exprime alors à l'aide d'une formule fermée :

$$q'_x(h) = (W + hK_x^T K_z)^{-1} W\hat{q},$$

où :

- $\hat{q}$: vecteur colonne des $\hat{q}_x$;
- W : matrice carrée diagonale de dimension m avec sur sa diagonale les w_x ;
- K_z : matrice de dimension $m - z \times m$ définie comme $\Delta^z q = K_z q$.

En pratique, le choix de la pondération qui intervient dans le critère de fidélité, s'effectue en posant $w_x = n_x$ avec n_x représentant le nombre d'entreprise total à la période $x = 1, ..., m$.

Dans les graphiques que nous retrouvons ci-dessous, nous avons les cas extrêmes de lissage (lorsque $h = 1$ et $h = 50$) ainsi que le cas retenu pour la modélisation. La difficulté du choix du h optimal est très complexe. En effet, il n'existe pas de méthode universelle permettant de sélectionner le lissage parfait. Néanmoins, il existe des méthodes à éviter :

- Prendre $h = 1$ reviendrait à accorder la même importance aux critères de fidélité et régularité. Cependant les deux phénomènes n'ont pas la même unité. En effet, d'une part $F(c)$ correspond à l'écart par rapport à la courbe des sinistres brutes (différence de fonctions mises au carré). D'autre part, $S(c)$ correspond à une somme de carré de dérivé de fonction d'ordre z. Le paramètre h permet alors de normaliser afin de pouvoir associer $S(c)$ et $F(c)$;
- Prendre $h = 50$ reviendrait à lisser fortement la courbe. Ce phénomène viendrait alors biaiser les valeurs de sinistralités qui ne concorderont plus aux observations.

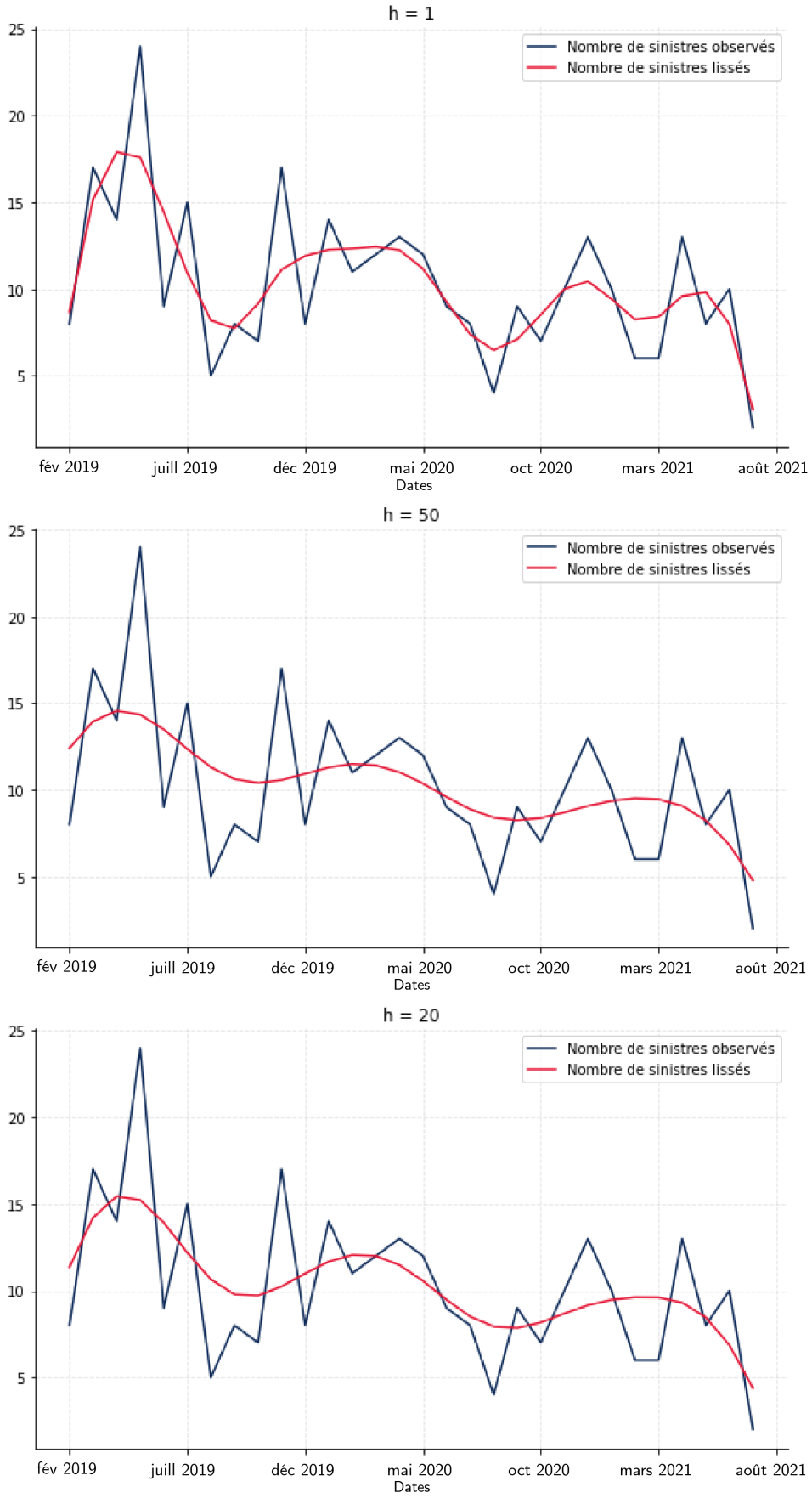

FIGURE 3.5 – Lissage de Whittaker-Henderson

Méthodologie suivie

Considérons un ensemble de paramètres candidats $\mathcal{H} = \{h_1, ..., h_k\} = \{1, 2, ..., 50\}$ avec $k = 50$. Nous avons dans un premier temps calculé les $q'_x(h_j)$ pour $j = 1, ..., k$.

Un test est alors proposé afin d'éliminer les candidats qui fournissent une très mauvaise adéquation. Ce test consiste à regarder pour tout j,

$$H_0 : q = q'(h_j),$$

contre

$$H_1 : q \neq q'(h_j).$$

Grâce à ce test, il est possible d'éliminer les courbes qui sont trop lisses et qui s'éloignent fortement des sinistres observés.

Sous H_0, la statistique de test s'exprime alors de la façon suivante :

$$D_n = \sum_{x=1}^{m} \frac{n_x}{\hat{q}_x(1-\hat{q}_x)}(\hat{q}_x - q'(h_j))^2.$$

Lorsque $D_n \longrightarrow 0$, alors $D_n \approx \chi^2(k)$ sous H_0.

Ce test permet de sélectionner un échantillon de courbe « acceptable » sous (H_0). Afin de sélectionner un unique h, nous avons effectué une analyse de sensibilité. Pour ce faire, nous avons choisi un candidat h. Puis, nous avons regardé si la courbe variait beaucoup lorsque nous utilisons $h + \epsilon$ avec ϵ petit. C'est alors que le choix de $h = 20$ a été opéré. Notons enfin que pour ce choix de h, trois cycles sont observés.

Modélisation de Lotka-Volterra

La première étape de la modélisation consista à lancer le modèle à l'aide de paramètres (a, b, c, d) initialisés arbitrairement. Quant aux nombres de proies et de prédateurs en $t = 0$ $(y1(0), y2(0))$, ils ont été initiés selon la sinistralité observée en $t = 0$. L'optimisation effectuée consista à chercher les paramètres du modèle qui minimisent la somme des écarts quadratiques entre la courbe lissée de Whittaker-Henderson et la courbe générée par les paramètres du modèle. Ce dernier nous renverra alors les paramètres « optimaux » en accord avec la fonction de perte.

Lorsque le modèle a été créé, le phénomène de base ne tenait pas compte d'une possibilité d'extinction de l'une des populations. Les paramètres utilisés dans la modélisation des deux dynamiques ont tendance à se compenser. C'est pourquoi, nous aurons toujours des courbes qui peuvent varier au cours du temps mais qui n'auront pas de tendance sur l'ensemble de la fenêtre d'observation. En effet, considérons une entreprise qui connaît son niveau de menace face au risque cyber. Elle prendra sûrement plusieurs mesures de sécurité sur du court terme faisant baisser à un instant donné les attaques. Cependant, cette dernière pourra également décider d'agir sur le long terme ce qui diminuera pérennement la sinistralité cyber. A l'aide de la figure 3.5, nous avons observé une tendance à la baisse de la sinistralité entre 2019 et 2021. C'est pourquoi, une deuxième étape consista à modifier les équations de Lotka-Volterra via l'ajout d'un paramètre e :

$$\begin{cases} \frac{dy_1(t)}{dt} = y_1(t)\big(a - by_2(t)\big); \\ \frac{dy_2(t)}{dt} = y_2(t)\big(-c + dy_1(t)\big). \end{cases} \quad \Longrightarrow \quad \begin{cases} \frac{dy_1(t)}{dt} = y_1(t)\big(a - by_2(t)\big) + et; \\ \frac{dy_2(t)}{dt} = y_2(t)\big(-c + dy_1(t)\big) - et. \end{cases} \tag{L-V2}$$

La dynamique du nombre d'attaques (prédateur) est représentée de la façon suivante :

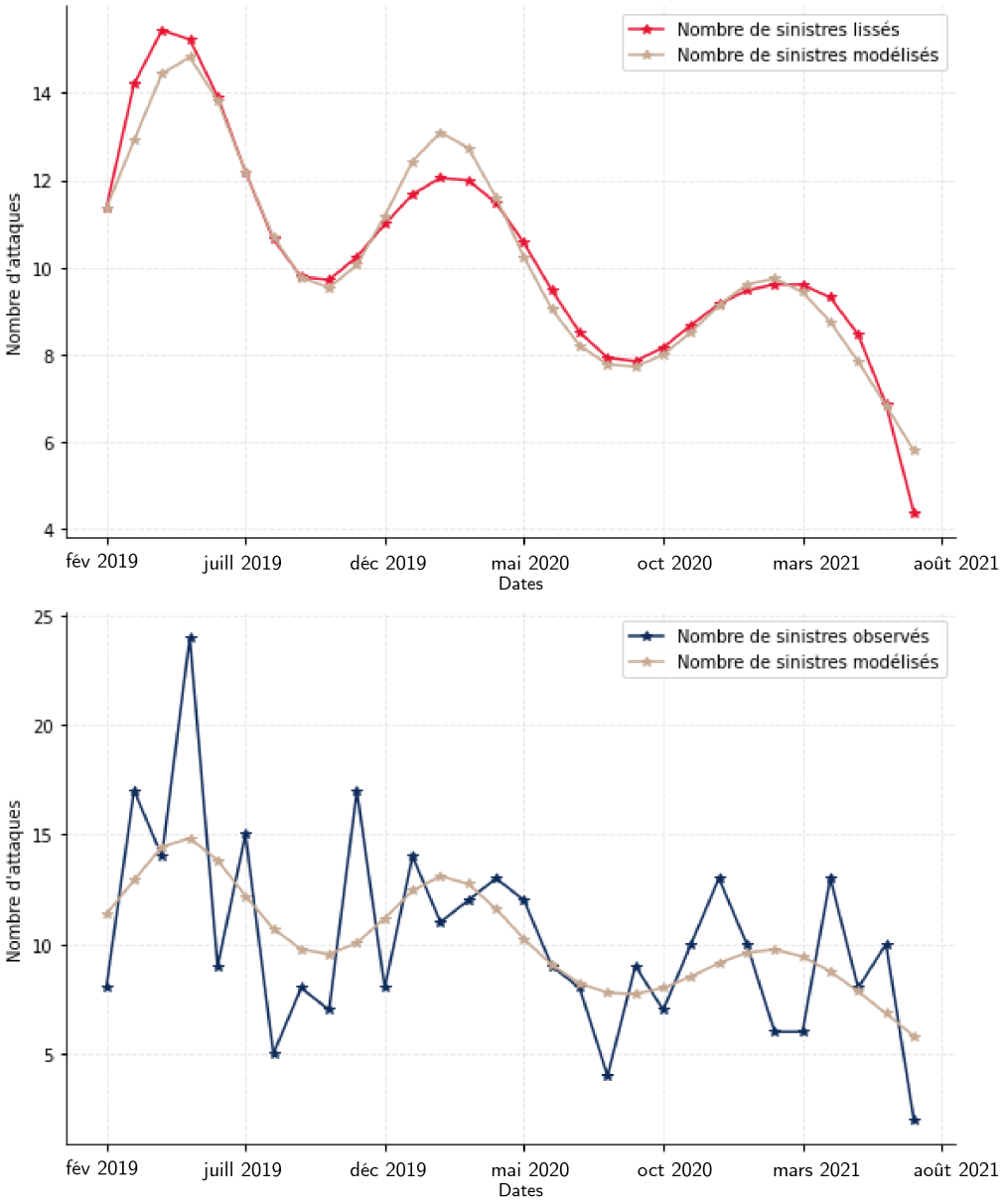

FIGURE 3.6 – Détermination de la dynamique du nombre d'attaques

Le nouveau modèle proie-prédateur modélise alors la sinistralité et l'indice de risque de la façon suivante :

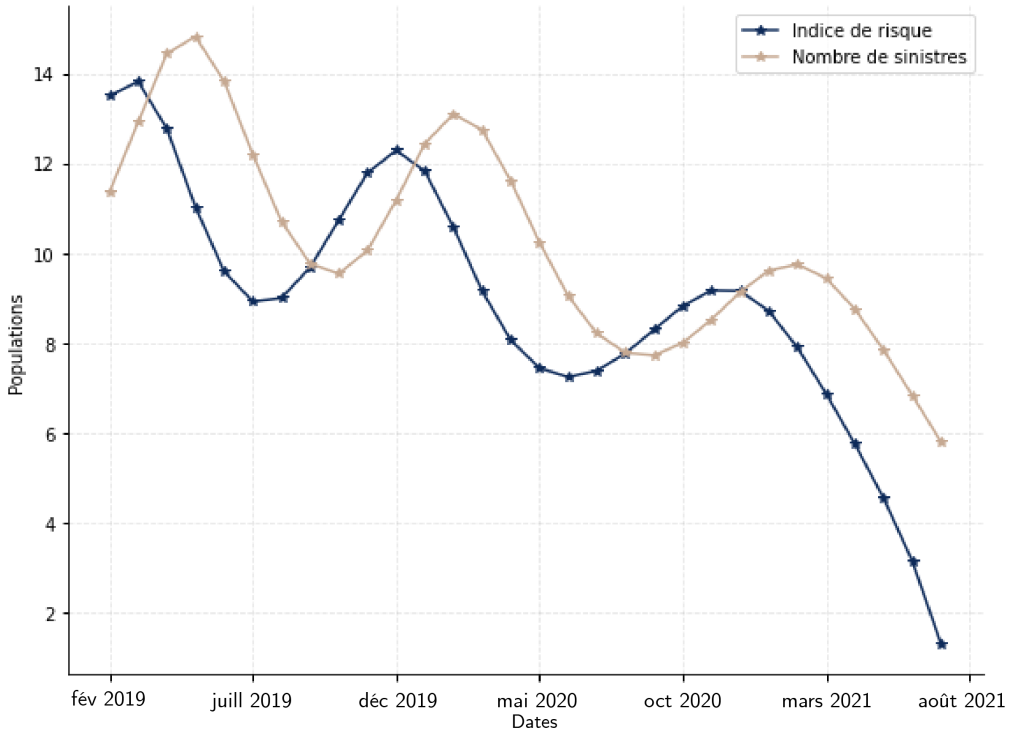

FIGURE 3.7 – Modèle de Lotka-Volterra amélioré

Au premier mois observé, c'est à dire en $t = 0$, l'indice de risque était plus élevé que la sinistralité. Cet indice décru entre le deuxième mois et le sixième mois. Cette diminution engendra une baisse du niveau de sinistralités avec un temps de « retard » mesuré à environ 2 mois. En effet, les entreprises étaient de moins en moins exposées face au risque cyber. De ce fait, le nombre de sinistres reporté était de plus en plus faible. Cependant, à partir du sixième mois, une hausse du niveau de risque a été constatée. Cette hausse permet d'anticiper une hausse de sinistralité future qui peut être due à un trop fort relâchement des entreprises sur les bonnes manières à adopter pour limiter les attaques cyber. Cette hausse d'indice de risque engendrera une hausse de sinistres avec un décalage de deux mois et ce jusqu'au onzième mois. Un cercle vertueux se forme alors. En effet, à partir du onzième mois, l'indice de risque des entreprises décroît, engendrant une baisse de sinistralité ... Cependant, notons toutefois que la tendance globale du phénomène nous montre que le niveau de sinistralité et l'indice de risque des entreprises décroît au fil des mois. Au vu des résultats observés, il serait possible de montrer que ces deux courbes tendent vers 0 (sous les hypothèses du modèle) sur une échelle de temps très grande.

Maintenant que l'indice de risque a été retrouvé, il est alors possible d'utiliser cette information dans un but tarifaire. En effet, grâce au modèle de Lotka-Volterra, il est possible de déterminer ainsi que de projeter l'indice de risque des assurés présent dans le portefeuille considéré. En récupérant ces éléments, la tarification peut être revu afin d'anticiper au mieux le comportement des assurés.

3.3 Tarification du modèle

3.3.1 Tarification théorique

Avant d'expliciter la méthodologie utilisée, procédons à un rappel de base sur ce qu'est la tarification d'une police d'assurance.

La méthode fréquence par coût est une façon courante de déterminer une première prime (prime pure notée π). En notant N le nombre total de sinistres cyber (fréquence) et Y le coût des sinistres associés (sévérité), la prime pure est déterminée de la façon suivante :

$$\pi = \mathbb{E}[N] \times \mathbb{E}[Y].$$

Afin que cette équation soit vérifiée, il faut préalablement supposer que Y est indépendant de N.

Pour d'obtenir la fréquence de sinistralité, c'est-à-dire $\mathbb{E}[N]$, il faudra exprimer cette dernière en fonction du nombre de sinistres ainsi que de l'exposition. En effet,

$$\mathbb{E}[N] = \frac{N}{E},$$

où E représente l'exposition. Cependant, dans le cadre de notre étude, il est difficile voire impossible de retracer l'exposition de chaque entreprise présente dans le portefeuille.

Quant à la détermination de $\mathbb{E}[Y]$, le coût moyen des sinistres est directement observable dans la base de données. En comparant les coûts des sinistres du portefeuille avec ce présentés par l'AMRAE, les sinistres qui composent le portefeuille sont de faibles sévérités car tous sont inférieurs à 300 000 €. Ci-dessous, une représentation des différents coûts (respectivement coûts des dommages globaux, coûts provisionnés initiaux et coûts de gestions de crise au global) a été effectuée.

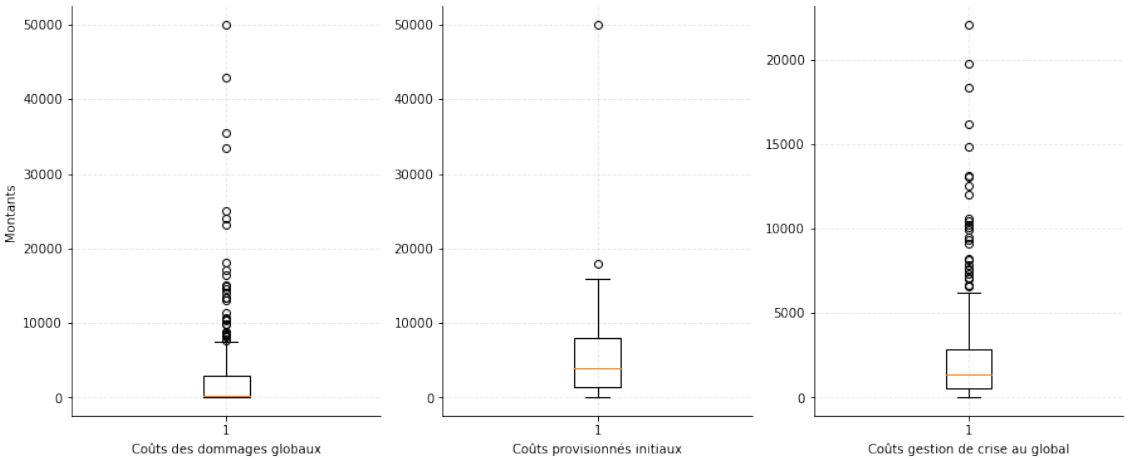

FIGURE 3.8 – Représentation des différents coûts par sinistre

Les coûts représentés ci-dessous sont homogènes. En effet, le montant des coûts varie entre 0 et 50 000 € pour les coûts provisionnés initiaux et les coûts liés aux dommages. Quant à ceux liés à la gestion de crise, ils varient entre 0 et 22 095 €. Il est également possible de constater que plus de 75% des sinistres du portefeuille répercutent des coûts qui sont inférieurs à

10 000 €. Avec les coûts présentés ci-dessus, nous allons pouvoir calculer et utiliser le coût moyen lors de la tarification sans faire des distinctions de cas. En effet, si notre base de données était composée de valeur extrême, il serait alors impossible de déterminer le coût moyen sans avoir préalablement séparer le cas « normal » du cas « extrême ».

Comme vu précédemment, il est peu recommandé de moyenner le coût des sinistres sans tenir compte du type de sinistres. C'est pourquoi, un coût moyen sera calculé selon chaque type d'attaques. En reprenant les notations précédentes, il est possible d'exprimer le coût moyen de la survenance d'un sinistre dans le portefeuille comme :

$$\mathbb{E}[Y] = \frac{1}{n}\sum_{i=1}^{n} Y_i.$$

Le tableau ci-dessous regroupe l'ensemble des $\mathbb{E}[Y]$ calculé pour chaque type d'attaques ainsi que pour différents coûts (coûts des dommages globaux, coûts provisionnés initiaux et coûts de gestion de crise au global).

TABLE 3.2 – Représentation des coûts moyens selon les types d'attaques

Type d'attaques	Dommages globaux	Provisionnés initialement	Gestion de crise au global
CRYPTOVIRUS	4 233,12 €	6 380,85 €	3 256,97 €
MALWARE	967,68 €	4 329,76 €	1 672,98 €
PHREAKING	700,90 €	2 555,56 €	971,00 €
PHISHING	227,48 €	1 190,98 €	651,52 €
ARNAQUE AVEC RANÇON	40,00 €	417,08 €	455,11 €
AUTRES	100,00 €	2 780,24 €	1 482,29 €
Moyenne	2 676,99 €	4 894,99 €	2 436,87 €

A l'aide du tableau ci-dessous, il est observé que le coût de sinistralité est très hétérogène en fonction du type d'attaques. En effet, le coût moyen des dommages pour la survenance d'un *cryptovirus* est de 4 233,12 € contre 40 € pour une arnaque avec rançon soit environ 104 fois mois élevé. Ce phénomène peut s'expliquer par la législation en vigueur. En effet, une police d'assurance cyber exclut dans la plupart des cas l'indemnisation d'une arnaque avec rançon si cette dernière a été payée par l'entreprise. C'est pourquoi, si l'entreprise n'a pas respecté les clauses du contrat, le coût du sinistre que l'assureur prendra à sa charge se verra fortement amoindri. Néanmoins, le coût moyen provisionné par l'assureur est toujours supérieur au coût moyen liés aux dommages globaux. Avec le régime prudentiel Solvabilité II, l'assureur est prudent et va toujours essayer de provisionner assez afin de faire face aux autres coûts qui peuvent survenir suite aux sinistres. Quant aux coûts liées à la gestion de la crise au global, ils sont du même ordre voire supérieur aux dommages en eux même. Prenons la cas d'une attaque de type *malware* : le coût moyen de gestion de crise représente 1 672,98 € contre un coût moyen de dommage de 967,68 € soit une différence de 705,30 €. Cet écart peut s'expliquer par la mobilisation requise afin de régler les dommages de cette attaque (appel à des équipes IT pour enlever le logiciel malveillant installé sur l'ordinateur, récupération des données, ou encore formatage du terminal). Enfin, il faut noter que les moyennes qui ont été calculées dans le tableau précédent tiennent compte des probabilités de survenance de chaque type d'attaques dans le portefeuille considéré.

L'indice de risque est complexe à traiter explicitement. Cependant, il est possible de faire un pont avec les modèles utilisés pour l'assurance des risques de catastrophes naturelles. En

effet, comme nous le verrons dans la section suivante, beaucoup de similitudes existent entre le cyber et les catastrophes naturelles. Nous pouvons citer comme exemple le caractère rare et sévère des évènements, les difficultés de définition et de scénarios en terme d'assurabilité, le montant d'indemnisation, ou encore les problèmes liés à la collecte/disponibilité de données.

3.3.2 L'assurance des risques de catastrophes naturelles

Définition

Contrairement au risque cyber, les risques de catastrophes naturelles sont définis par le Code des Assurances comme « les dommages matériels directs non assurables ayant eu pour cause déterminante l'intensité anormale d'un agent naturel, lorsque les mesures habituelles à prendre pour prévenir ces dommages n'ont pu empêcher leur survenance ou n'ont pu être prises » (article L125-1 du Code des Assurances). Cependant, cette définition reste floue et ne détaille pas de manière explicite les critères permettant de qualifier si un événement est classé comme catastrophe naturelle. De ce fait, nous pouvons dans cette étude considérer que tout évènement naturel de forte intensité peut être considéré comme évènement catastrophe naturelle.

Afin que le risque catastrophe naturelle soit considéré comme assurable, il doit être considéré comme aléatoire, quantifiable et mutualisable. Pour le caractère aléatoire, ce point pourrait être considéré comme trivial auparavant. Néanmoins, avec le dérèglement climatique, nous observons de plus en plus d'évènements catastrophiques, ce qui pousse à remettre en question cette notion d'aléa. La mutualisation et la quantification de ce dernier n'est pas pour autant plus simple à observer. En effet, le risque lié au catastrophe naturelle est caractérisé par :

- une volatilité très forte dû à une très forte variation des évènements climatiques ;
- une grosse queue de distribution dû à l'hétérogénéité des sinistres ;
- un historique de sinistralité n est assez faible. En effet, comme pour le risque cyber, il est difficile d'avoir accès à une base de données conséquente afin de mener des analyses robustes ;
- la rareté d'un événement. Les évènements liés au risque de catastrophe naturelle ne se produisent pas à chaque instant.

Cependant, en France, la législation impose à chaque contrat d'assurance dommage de dédier une part de la prime aux catastrophes naturelles : ce phénomène permet d'assurer une certaine mutualisation (ce qui n'est pas le cas pour les garanties cyber).

Les risques liés aux catastrophes naturelles peuvent être considérés comme « non assurables » de part leur fréquence faible mais leur impact important rendant complexe la modélisation. En France, l'assurance couvrant ce type d'évènements est régi par un régime d'indemnisation des catastrophes naturelles ou « régime CatNat ».

Régime d'indemnisation *CatNat*

Le régime d'indemnisation des catastrophes naturelles ou « régime CatNat » a été mis en place en 1982 afin d'assurer les événements naturels rares et très coûteux. Nous ne nous attarderons ici sur le détail des évolutions qu'a connu ce régime au fil des années.

Cependant, nous allons essentiellement parlé d'une réforme qui est intervenue dans les années 2000. Selon l'article L125-2 du Code des Assurances, le taux annuel de la prime ou cotisation relative à la garantie contre les effets des catastrophes naturelles est fixé à :

- 6% des primes ou cotisations afférentes aux garanties vol et incendie, ou, à défaut, 0,5% des primes ou cotisations afférentes aux garanties dommages pour les contrats automobile ;
- 12% des primes ou cotisations afférentes aux garanties dommages sur les autres contrat.

Il faut également souligner le fait que les taux ci-dessus sont calculés sur les primes ou cotisations nettes de toutes taxes.

3.3.3 Application à l'assurance cyber

Une alternative tarifaire proposée est la suivante :

- Étape 1 : retracer dans notre base de données le chiffre d'affaire par entreprise selon la variable CSP ;
- Étape 2 : normaliser l'indice de risque afin qu'il appartienne à l'intervalle $[0, 1]$;
- Étape 3 : appliquer un taux au chiffre d'affaire (semblable à ce qui est fait pour les catastrophes naturelles) et déterminer la prime pure de chaque entreprise selon les 3 points précédents.

Étape 1

Dans la base de données initiale (appelé « base 0 »), outre la catégorie socio-professionnelle (CSP) et le métier exercé par l'entreprise, aucune information n'est disponible à propos du chiffre d'affaire. Cependant, une seconde base de données (appelé « base 1 ») de ce même assureur répertorie les chiffres d'affaires de certains de ses assurés selon le libellé de la CSP. Nous avons calculé dans un premier temps la moyenne des chiffres d'affaires par CSP dans la base 1. Puis, nous l'avons ventilé dans la base 0 selon la maille CSP.

Étape 2

Comme présenté précédemment, l'indice de risque déterminé par le modèle de Lotka-Volterra est à valeur dans $\mathbb{R}^+$. En effet, lors du calcul de ce dernier, nous avons considéré l'ensemble des entreprises exposées car nous avons repris l'ensemble des sinistres. Or, nous aimerions nous ramener à une tarification individuelle. C'est pourquoi, nous voudrions obtenir un indice de risque individuel. Comme nous ne disposons pas de toutes les informations permettant de retracer l'exposition des entreprises, nous allons devoir prendre des hypothèses sur ce point, d'où les choix ci-dessous de méthode de normalisation. Une première solution serait de ramener l'indice de risque dans l'intervalle $[0, 1]$. Une technique simple pour ramener les scores bruts (x) dans cet intervalle serait d'utiliser une fonction :

$$\begin{array}{rccc} \phi_1 & : & \mathbb{R}^+ & \to & [0,1], \\ & & x & \mapsto & \frac{x-min(x)}{max(x)-min(x)}. \end{array}$$

Mais, si le problème d'interprétation du score est résolu, le problème de la disparité des distributions des valeurs persiste. Une multitude de méthode alternative permet également

de ramener ce score entre 0 et 1. Deux autres méthodes ont été utilisées dans cette étude :

$$\begin{array}{rccc} \phi_2 & : & \mathbb{R}^+ & \to & [0,1], \\ & & x & \mapsto & \frac{x}{||x||_2}. \end{array}$$

$$\begin{array}{rccc} \phi_3 & : & \mathbb{R}^+ & \to & [0,1], \\ & & x & \mapsto & \frac{x}{10^{\lfloor log_{10}(max(x))+1 \rfloor}}. \end{array}$$

Après application de ces différentes méthodes de normalisation, nous obtenons le graphique suivant :

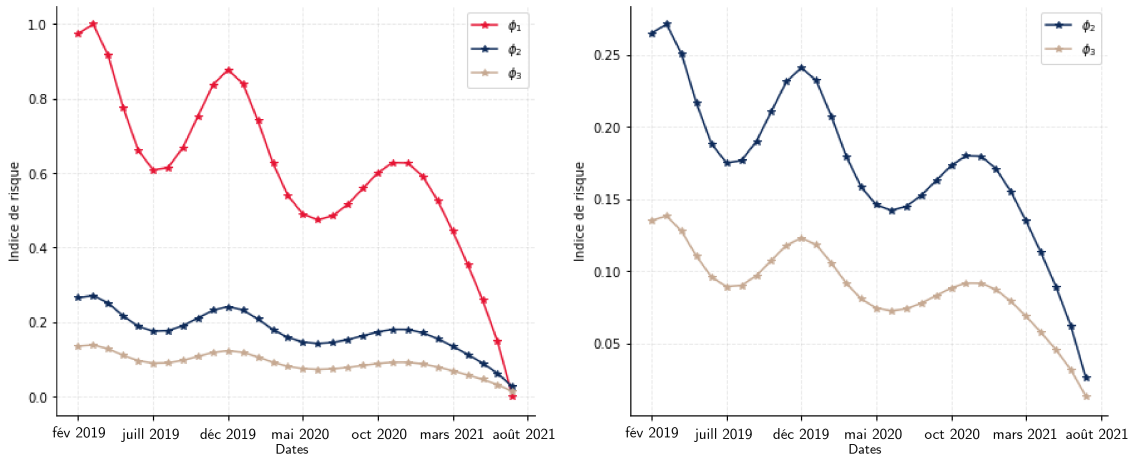

FIGURE 3.9 – Normalisation de l'indice de risque cyber

D'après le premier graphique ci-dessus, la première technique de normalisation (ϕ_1) suppose que le minimum ainsi que le maximum sont atteint dans cette fenêtre d'observation. Cela a pour avantage de disperser les indices de risque entre 0 et 1. Cependant, en supposant que le maximum (respectivement le minimum) est atteint sur l'intervalle de temps considéré, cela reviendrait à dire que les entreprises n'auront jamais un indice de risque plus élevé (respectivement plus bas) à l'avenir. Enfin, le fait d'atteindre les bornes poseraient également un problème dans la tarification car il s'agirait de cas extrême et purement théorique. La troisième technique de normalisation (ϕ_3) permet, quant à elle, de regrouper les variables dans un intervalle assez restreint. En effet, après application de cette méthode sur le jeux de données, l'écart entre l'indice maximum et minimum est de seulement 13 points de pourcentages. Cette méthode aura pour avantage de laisser un plus large éventail de possibilité à une évolution future de l'indice de risque. Cependant, afin de déterminer une prime sur la fenêtre de temps considérée, l'écart entre chaque indice n'est pas assez significatif pour différencier les primes. C'est pourquoi, la seconde technique a été choisie pour la suite de l'étude. Cette méthode aura d'une part l'avantage de ne pas atteindre les bornes, de permettre une certaine dispersion entre chaque indice de risque cyber (25 points de pourcentages entre le maximum et le minimum) ainsi que de permettre un large éventail de possibilité à une évolution future de l'indice de risque.

Étape 3

Une fois que toutes les variables ont été identifiées et traitées, il est alors possible de déterminer la prime pure de la façon suivante :

Soient :

- ent_j l'entreprise j ;
- $C(ent_j)$ le chiffre d'affaire de l'entreprise j ;
- i le taux annuel prélevé sur le chiffre d'affaire constant ;
- $\phi(x)$ l'indice de risque cyber de l'entreprise j.

Alors, la prime est déterminée par :

$$\pi(ent_j) = i \times C(ent_j) \times \phi(x).$$

Cependant, aucune réglementation (contrairement au régime *CatNat*) ne prévoit un montant de taux. C'est pourquoi, nous avons réalisé une étude de sensibilité et regardé l'impact sur le rapport de sinistre à prime au niveau global (toutes entreprises confondues).

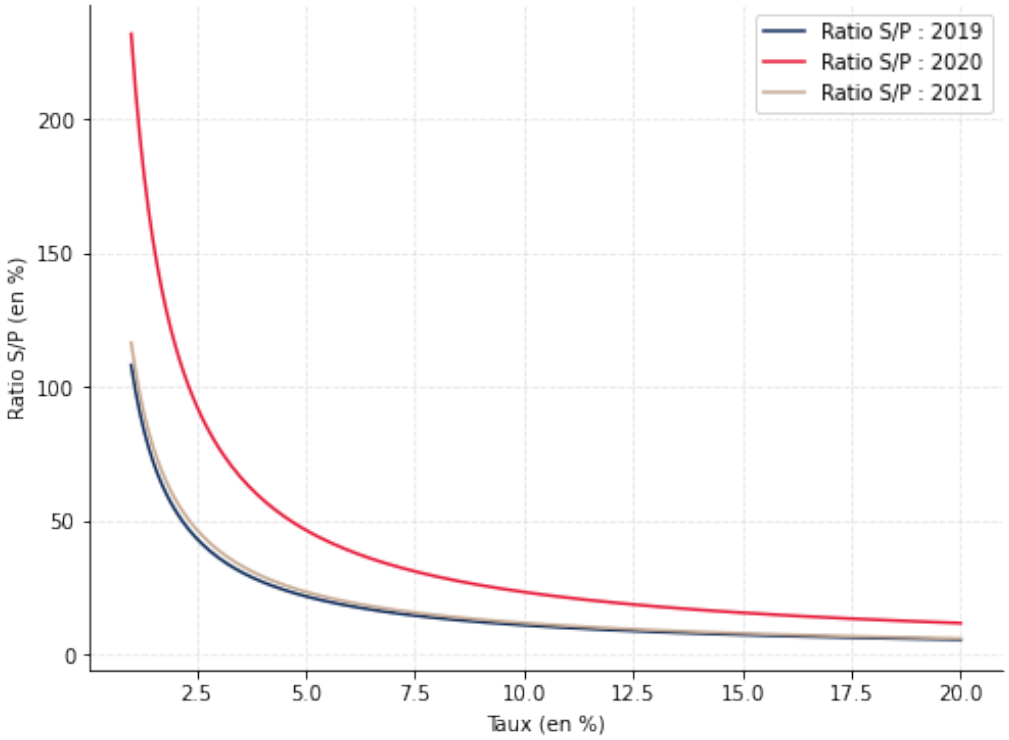

FIGURE 3.10 – Représentation des S/P globaux en fonction du taux appliqué

Ce graphique est à mettre en lumière avec l'étude de l'AMRAE présentée dans le chapitre 1 (1.3). En prenant le même niveau de S/P en 2019 que présenté dans le rapport LUCY (84%), nous obtenons un taux de 1,30%. Alors, au niveau du portefeuille au global la représentation est la suivante :

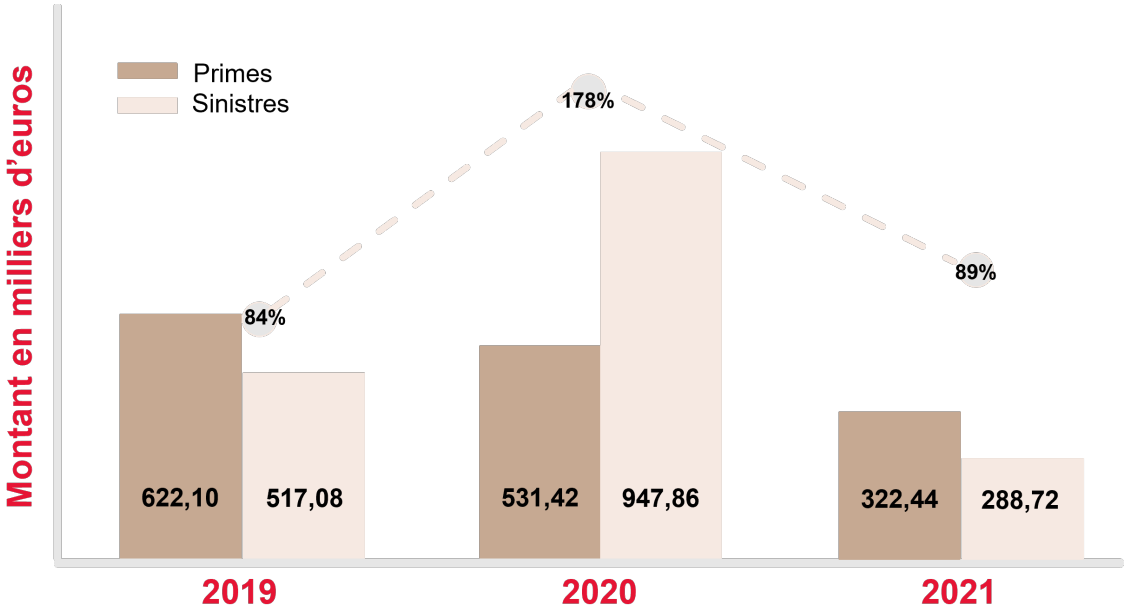

FIGURE 3.11 – Représentation des S/P globaux avec un taux de 1,30%

Selon le graphique précédent, nous constatons une diminution du volume de primes de 15 %, qui est passé de 622,10 k€ en 2019 à 531,42 k€ en 2020. Mais cette décroissance est très inférieure à celle du montant des indemnisations versées qui a été multiplié par 1,8, passant de 517,08 k€ en 2019 à 947,86 k€ en 2020. Pour les assureurs, le ratio Sinistres sur Primes (S/P) est donc passé de 84% à 178%. Ces données permettent de mieux comprendre la saturation que connaît le marché de l'assurance cyber. Les entreprises bénéficient de réduction tarifaire en 2020 avec un volume de sinistre qui croît impactant la solvabilité des assureurs. Ce phénomène est principalement dû à la crise sanitaire en 2020 que nous avons explicité précédemment dans le chapitre 1. En effet, lorsque nous regardons le début d'année 2021, nous observons que le volume globale des primes est supérieur à celui des indemnisations. De ce fait, le ratio S/P est passé de 178% en 2020 à 89% en 2021 soit une diminution de 89 points de pourcentages.

TABLE 3.3 – Représentation des S/P selon le type de métiers

Type de métiers	2019	2020	2021
PROFESSIONNEL	127%	198%	40%
ENTREPRISE	78%	53%	112%
COLLECTIVITE	381%	618%	176%
AGRICOLE	27%	155%	58%
CONSTRUCTION	147%	109%	132%
ASSOCIATION	132%	255%	1135%

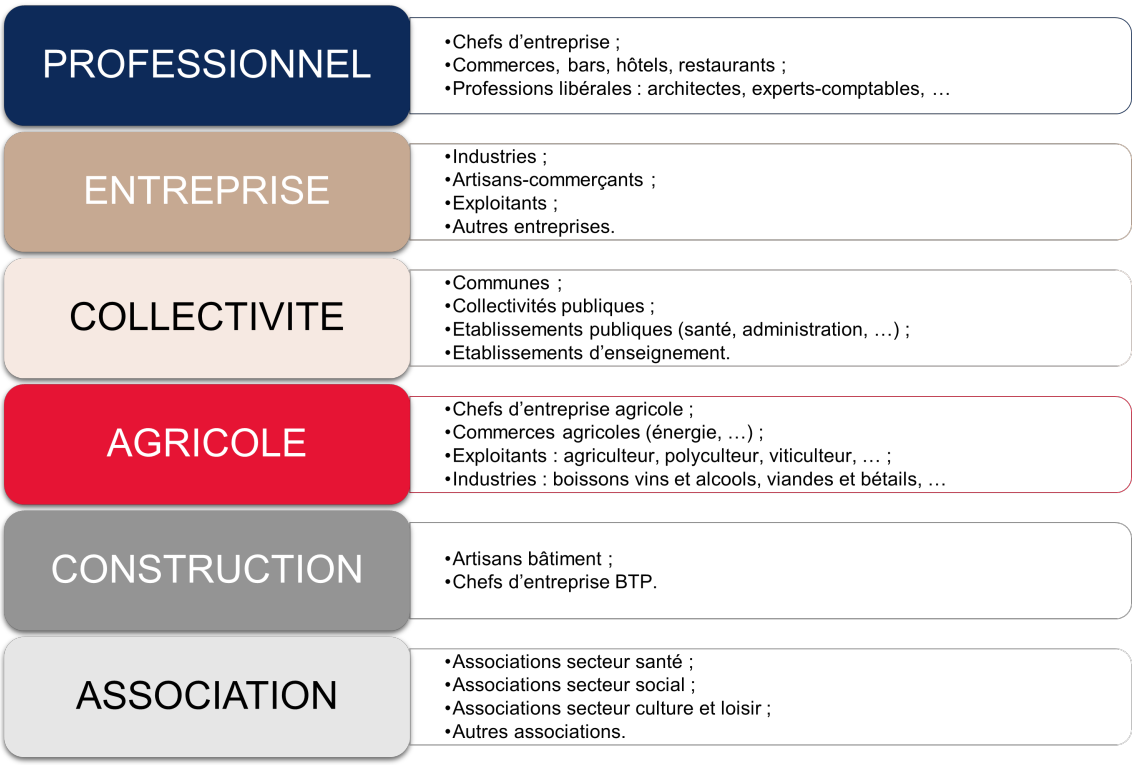

FIGURE 3.12 – Descriptions des métiers

A l'aide du tableau ci-dessus, lorsque nous regardons selon la maille métier, le montant des S/P est très disparate d'une entité à l'autre. Ceci peut s'expliquer de par le descriptif de métier ci-dessus. Les métiers ayant le plus fort S/P entre 2019 et 2021 sont les collectivités ainsi que les associations. Les collectivités rassemblent les communes, les établissements publiques ou encore les établissements scolaires. Nous pourrions considérer que ces organisations ne se soucieraient pas en priorité des problématiques liées au risque cyber. En effet, prenons pour exemple un hôpital ou encore la mairie d'un petit village. Le but premier de ces deux organisations ne sera pas de disposer de la meilleure mise à jour de leur système informatique. De plus, la plupart de ces organisations ne disposent pas d'une équipe informatique dédiée à la sécurité informatique. Ce sont donc des personnes peu voire non formées, qui ne connaissent pas les risques liés au cyber et qui doivent s'occuper de ces problématiques. Cependant, ce phénomène n'explique pas entièrement les forts niveaux des S/P. Rappelons que ces niveaux ont été obtenus à l'aide du calcul des primes que nous avons effectué précédemment avec le modèle de Lotka-Volterra. La tarification réalisée ne tenait seulement compte du chiffre d'affaire de l'entreprise et non pas du type de métier considéré. De ce fait, une amélioration du modèle pourrait être proposée en prenant en compte par exemple le métier comme variable explicative et en appliquant à notre prime un coefficient ρ qui différera selon le métier considéré.

3.4 Sensibilité et impacts des hypothèses choisies

Toutes les hypothèses que nous avons faites durant ce travail pourraient être remises en questions. C'est pourquoi, une partie sur la sensibilité et leurs impacts a été réalisée.

Une grande limite est néanmoins à souligner : nous disposons d'une base de données de **sinistrés**. De ce fait, tous les S/P ainsi que les primes présentés durant cette étude regroupe l'ensemble des assurés sinistrés exclusivement.

3.4.1 Sensibilité des paramètres

Hypothèse sur le paramètre de lissage (h)

A l'aide de la figure 3.5, nous avons pris comme hypothèse que le lissage de Whittaker-Henderson devait respecter à la fois le critère de fidélité (refléter au mieux la sinistralité brute) ainsi que le critère de régularité (lisser au mieux la courbe). Nous avons supposé $h = 20$ après avoir réalisé des tests. Cependant, comment aurait été le modèle si nous avions choisi $h = 10$ ou $h = 30$?

Lorsque $h = 10$, le critère de Whittaker-Henderson s'exprime de la façon suivante :

$$WH_{10}(c) = F(c) + 10S(c).$$

La sinistralité brute est moins bien lissée. De ce fait, comme nous le montre le graphique ci-dessous, le modèle de Lotka-Volterra aurait plus de difficulté à ce calibrer. Afin de calibrer les paramètres du modèle, nous devons minimiser la somme des écarts quadratiques entre la vraie courbe et celle générée par des paramètres initiaux. Cependant, cette minimisation devient « plus compliquée » sur des courbes non lisses.

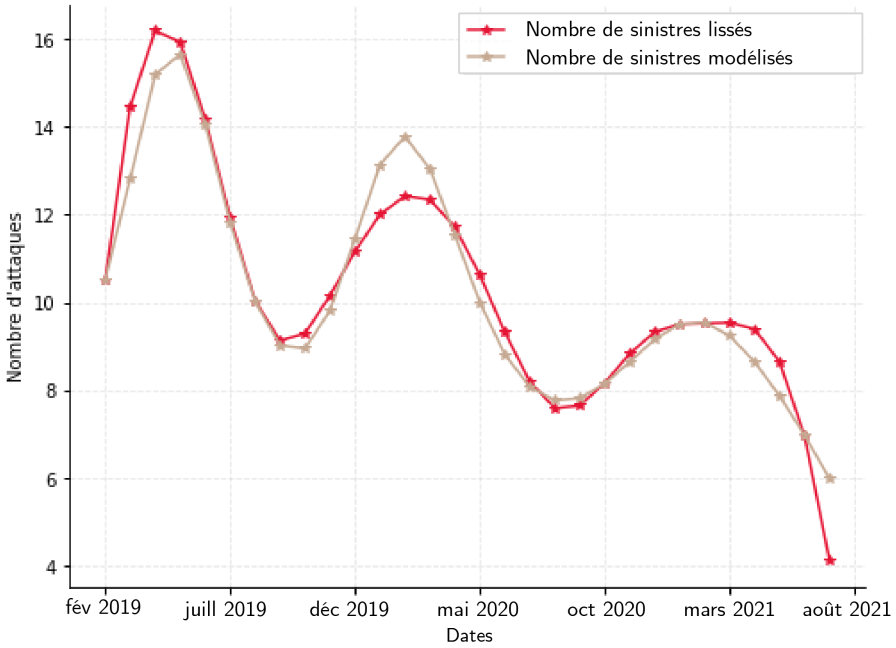

FIGURE 3.13 – Modélisation de la sinistralité avec le modèle de Lotka - Volterra

À partir de la sinistralité qui a été reconstruite par la dynamique des prédateurs, la détermination de l'indice de risque est représentée ci-dessous.

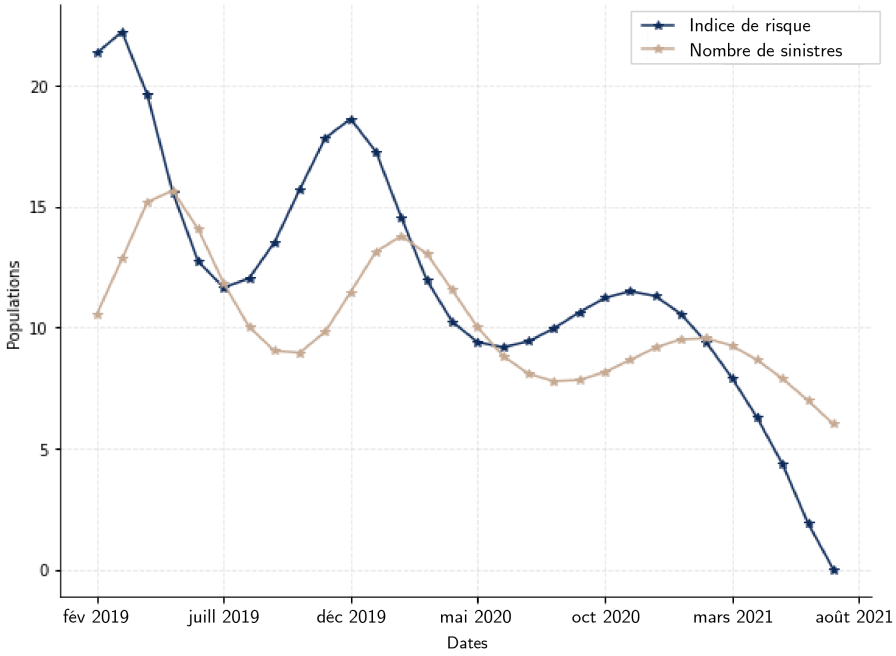

FIGURE 3.14 – Modèle de Lotka - Volterra

TABLE 3.4 – S/P par scénario ($h = 10$) selon le type de métiers

Type de métiers	2019	2019 sc.1	2020	2020 sc.1	2021	2021 sc.1
PROFESSIONNEL	127%	↑ 4pts	198%	↑ 2pts	40%	↓ 1pt
ENTREPRISE	78%	↓ 1pt	53%	↓ 1pt	112%	↑ 2pts
COLLECTIVITE	381%	= 0pt	618%	↑ 19pts	176%	↑ 7pts
AGRICOLE	27%	= 0pt	155%	↓ 2pts	58%	↑ 3pts
CONSTRUCTION	147%	↓ 2pts	109%	↑ 1pt	132%	↑ 8pts
ASSOCIATION	132%	↑ 1pt	255%	↑ 5pts	1135%	↑ 34pts

L'impact sur le ratio combiné commence à se faire ressentir à partir de 2020. Lorsque nous regardons à la maille métier, le S/P professionnel, entreprise ou encore agricole reste assez stable dans le temps malgré le choc. Quant au S/P collectivité, construction et association, il fluctue beaucoup plus en raison de leur niveau élevé.

Lorsque $h = 30$, le critère de Whittaker-Henderson s'exprime de la façon suivante :

$$WH_{30}(c) = F(c) + 30S(c).$$

La sinistralité brute est très bien lissée. De ce fait, comme nous le montre le graphique ci-dessous, le modèle de Lotka-Volterra aurait plus de facilité à ce calibrer. Cependant, considérer un paramètre de lissage trop important éloignera les nouveaux obtenus de la sinistralité réelle.

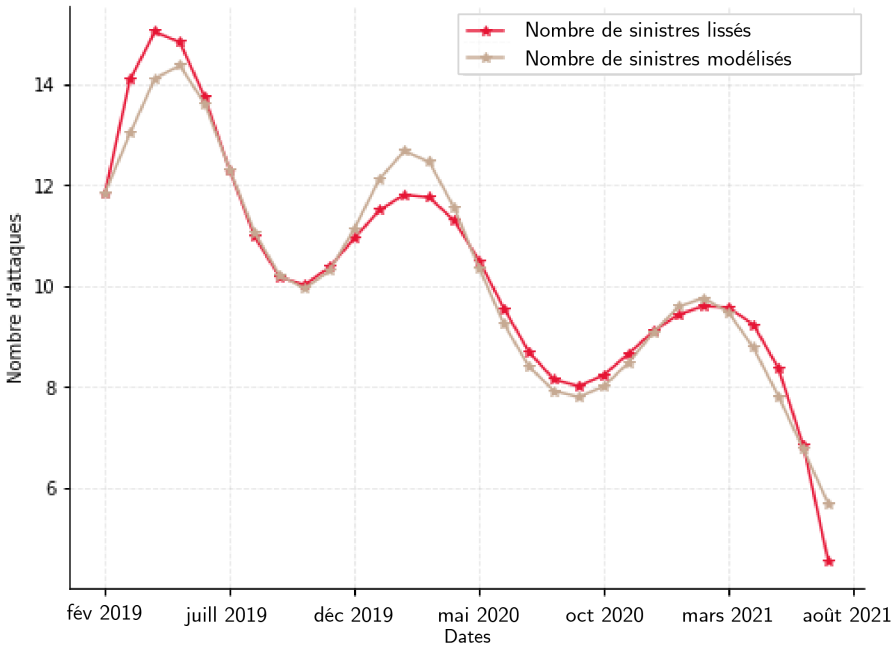

FIGURE 3.15 – Modélisation de la sinistralité avec le modèle de Lotka - Volterra

A partir de la sinistralité qui a été reconstruite par la dynamique des prédateurs, la détermination de l'indice de risque est représentée ci-dessous.

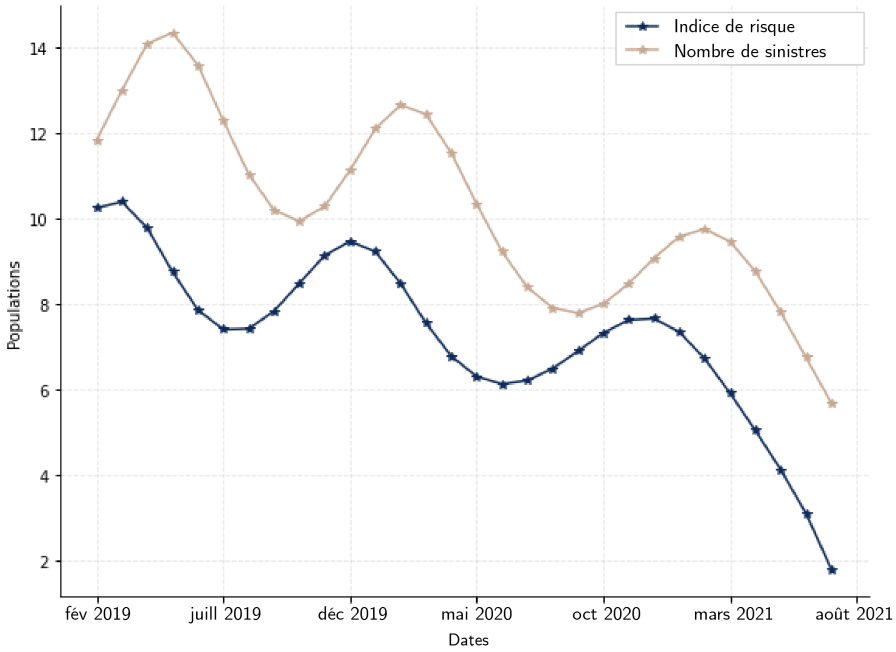

FIGURE 3.16 – Modèle de Lotka - Volterra

TABLE 3.5 – S/P par scénario ($h = 30$) selon le type de métiers

Type de métiers	2019	2019 sc.1	2020	2020 sc.1	2021	2021 sc.1
PROFESSIONNEL	127%	↓ 2pts	198%	↓ 1pt	40%	= 0pt
ENTREPRISE	78%	↑ 1pt	53%	↑ 1pt	112%	= 0pt
COLLECTIVITE	381%	= 0pt	618%	↓ 6pts	176%	↓ 2pts
AGRICOLE	27%	= 0pt	155%	↑ 1pt	58%	↓ 1pt
CONSTRUCTION	147%	↑ 1pt	109%	↓ 1pt	132%	↓ 2pts
ASSOCIATION	132%	↓ 1pt	255%	↓ 4pts	1135%	↓ 7pts

Ici, au niveau global, le changement du paramètre de lissage n'affecte pas drastiquement le S/P des différents métiers. Notons toutefois que les variations les plus importantes se situent pour les collectivités ainsi que les associations.

En conclusion, ne pas lisser la courbe engendre une « assez forte » variation du S/P. Cependant, un lissage excessif n'aura, quant à lui, assez peu d'impact sur le ratio combiné.

Hypothèses sur la courbe des proies - indice de risque

Le modèle de Lotka-Volterra nous fournit une unique courbe retraçant l'indice de risque. Cependant, nous pouvons faire des hypothèses statistiques afin de considérer non plus une unique courbe mais plutôt un scénario *up* ainsi qu'un scénario *down* autour de cette courbe. Pour cela, considérons le cadre suivant :

- Soit X le nombre de sinistres déterminé à partir du modèle de Lotka-Volterra ;
- Supposons $X = (X_i)_{i \in [\![0,29]\!]} \sim \mathcal{P}(\lambda), \lambda > 0$;
- Nous avons $\mathcal{P}(\lambda) \approx \mathcal{N}(\lambda, \lambda)$.

Dans la suite du paragraphe, nous allons considérer les deux scénarios (*up* et *down*). De ce fait, le modèle proie-prédateur est représenté de la façon suivante :

Indice de risque Nombre de sinistres

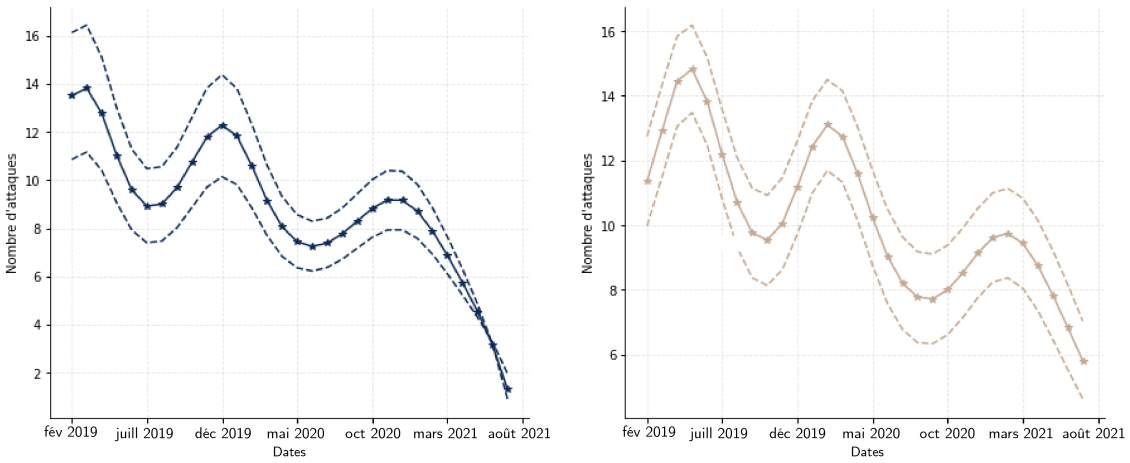

FIGURE 3.17 – Application des différents scénarios sur le modèle de Lotka - Volterra

En notant les scénarios comme ci-dessous, nous obtenons le tableau suivant :

- Scénario 1 : $X_i \leftarrow X_i - 1,96 \times \sqrt{\frac{\lambda}{n}}$;
- Scénario 2 : $X_i \leftarrow X_i + 1,96 \times \sqrt{\frac{\lambda}{n}}$.

TABLE 3.6 – Représentation des S/P par scénarios selon le type de métiers

Type de métiers	2019	2019 sc.1	2019 sc.2	2020	2020 sc.1	2020 sc.2	2021	2021 sc.1	2021 sc.2
PROFESSIONNEL	127%	↓ 1pt	= 0pt	198%	= 0pt	= 0pt	40%	= 0pt	= 0pt
ENTREPRISE	78%	= 0pt	= 0pt	53%	= 0pt	= 0pt	112%	↓ 1pts	= 0pt
COLLECTIVITE	381%	= 0pt	= 0pt	618%	↓ 4pts	↑ 4pts	176%	↓ 2pts	↑ 1pt
AGRICOLE	27%	= 0pt	= 0pt	155%	↑ 1pt	= 0pt	58%	↓ 1pt	↑ 1pt
CONSTRUCTION	147%	= 0pt	= 0pt	109%	↑ 1pt	↓ 1pt	132%	↓ 2pts	↑ 2pts
ASSOCIATION	132%	↓ 1pt	↑ 1pt	255%	↓ 2pts	↑ 1pt	1135%	↓ 7pts	↑ 6pts

Avoir considéré ces deux scénarios nous conforte sur le fait suivant : changer de courbe n'a que peu d'impact sur le S/P.

Hypothèse sur le choix de fonction de normalisation

Lorsque nous avons élaboré notre méthode de tarification, nous avons sélectionné comme fonction de normalisation (ϕ_2) celle qui permettait à la fois de disperser l'indice de risque mais sans pour autant atteindre les bornes [0, 1]. Cependant, que serait-il passé si nous avions choisi la fonction ϕ_1 ou ϕ_3 ? C'est pourquoi, nous allons voir dans ce paragraphe l'impact d'un changement de normalisation sur le S/P.

Considérons deux scénarios :

- Scénario 1 :

$$\begin{array}{rccc} \phi_1 & : & \mathbb{R}^+ & \rightarrow & [0,1], \\ & & x & \mapsto & \frac{x-min(x)}{max(x)-min(x)}. \end{array}$$

- Scénario 2 :

$$\begin{array}{rccc} \phi_3 & : & \mathbb{R}^+ & \rightarrow & [0,1], \\ & & x & \mapsto & \frac{x}{10^{\lfloor log_{10}(max(x))+1 \rfloor}}. \end{array}$$

TABLE 3.7 – S/P par scénarios selon le type de métiers

Type de métiers	2019	2019 sc.1	2019 sc.2	2020	2020 sc.1	2020 sc.2	2021	2021 sc.1	2021 sc.2
PROFESSIONNEL	127%	↑ 3pts	↑ 2pts	198%	↑ 79pts	↑ 68pts	40%	↑ 88pts	↑ 77pts
ENTREPRISE	78%	↑ 1pt	↑ 1pt	53%	↑ 20pts	↑ 18pts	112%	↑ 255pts	↑ 215pts
COLLECTIVITE	381%	↑ 5pts	↑ 5pts	618%	↑ 243pts	↑ 213pts	176%	↑ 403pts	↑ 337pts
AGRICOLE	27%	= 0pt	= 0pt	155%	↑ 60pts	↑ 53pts	58%	↑ 136pts	↑ 112pts
CONSTRUCTION	147%	↑ 1pt	↑ 2pts	109%	↑ 44pts	↑ 37pts	132%	↑ 313pts	↑ 252pts
ASSOCIATION	132%	↑ 2pts	↑ 2pts	255%	↑ 108pts	↑ 88pts	1135%	↑ 2585pts	↑ 2175pts

Changer la méthode de normalisation aura un très fort impact sur les S/P. Après avoir calibrés les scénarios sur 2019, lorsque nous regardons pour 2020, nous apercevons des écarts de l'ordre de centaines de points de pourcentages pour les collectivités ainsi que les associations.

3.4.2 Qui devons-nous cibler ?

Et si nous ciblons seulement des entreprises ayant un chiffre d'affaire supérieur à un certain seuil ?

Supposons que le seuil retenu soit de 1 million d'euros. De ce fait, nous excluons de notre portefeuille toutes les petites entreprises ayant un chiffre d'affaire inférieur au seuil choisi. Ces dernières disposent d'un faible niveau de prime (au vu de la méthode de tarification élaborée précédemment). Mais, elles peuvent contracter un fort niveau de sinistralité, ceci impactant le S/P.

Ci-dessous, nous retrouvons le niveau du S/P global sans les petites entreprises.

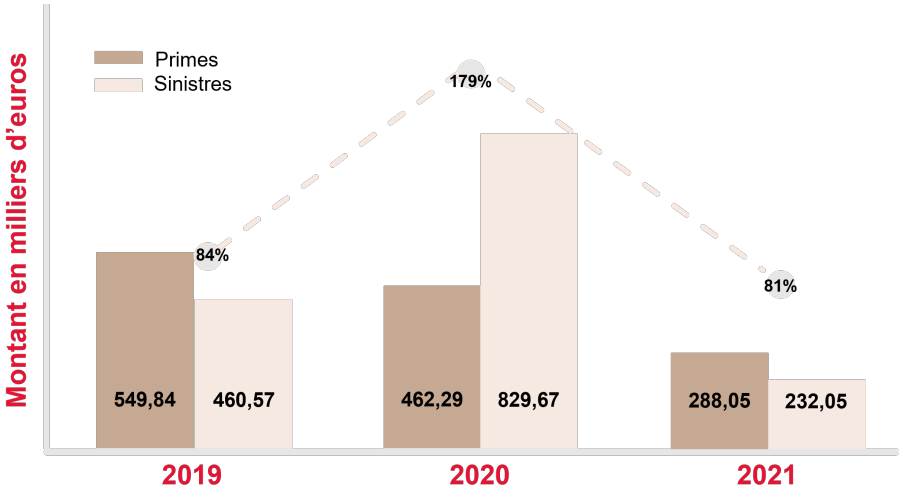

FIGURE 3.18 – S/P portefeuille sans les petites entreprises

Enlever les entreprises ayant un chiffre d'affaire inférieur de notre portefeuille permettrait, toute chose égale par ailleurs d'améliorer le ratio combiné de 9 points de pourcentages en 2021. Cependant, il est également constaté une hausse d'un point de pourcentage pour 2020 du S/P.

Et si nous excluons les entreprises qui pratiquent un certain métier ?

Comme nous l'avons vu précédemment, il existe une grande disparité au niveau du S/P en fonction du métier que l'entreprise exerce. Ce phénomène pourrait s'expliquer principalement par le niveau informatique que ces dernières disposeraient ainsi que des données qui seraient utilisées. C'est pourquoi, les collectivités ainsi que les associations auront tendance à se faire fortement attaquer comparé à d'autres entreprises. Un assureur peut donc choisir s'il compte assurer ou non les métiers qui, lui engendrerait probablement une forte sinistralité. C'est pourquoi, nous allons voir dans ce paragraphe l'impact sur le S/P global si nous retirons certains métiers de notre portefeuille (notamment les collectivités et les associations).

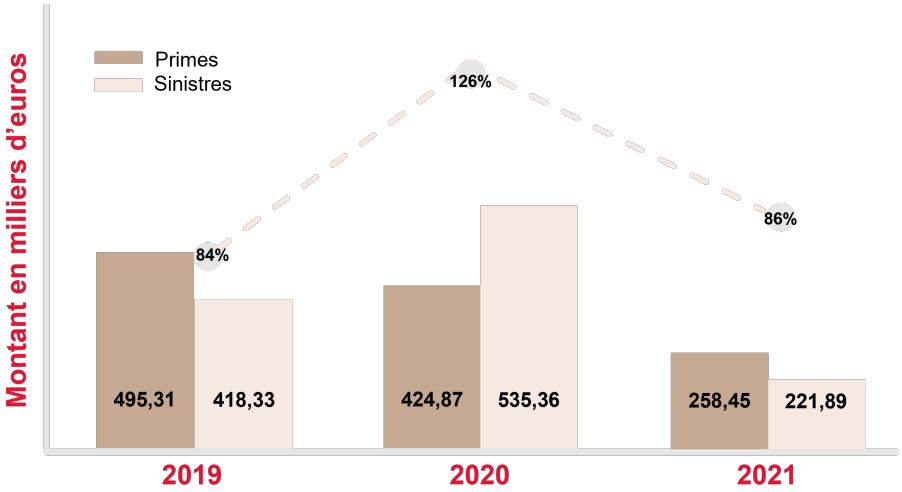

FIGURE 3.19 – S/P portefeuille sans les associations et les collectivités

Ne pas assurer les associations ainsi que les collectivités viendraient améliorer le S/P sur 2020 ainsi que 2021. En effet, le S/P 2020 était de 178% contre 126% pour ce nouveau portefeuille soit un gain de 52 points de pourcentages. Il en va de même avec le S/P en 2021 représentant un gain de 4 points de pourcentage par rapport au scénario central.

Et si nous excluons certains types d'attaques ?

D'après le tableau 3.2, nous avons vu que le coût d'indemnisation variait drastiquement selon le type d'attaque que subissait l'entreprise. C'est pourquoi, nous pourrions imaginer exclure du contrat la couverture de certaines attaques comme les cryptovirus ou encore les logiciels malveillants de type *malware*. Si cela est fait, alors nous obtenons les résultats suivants :

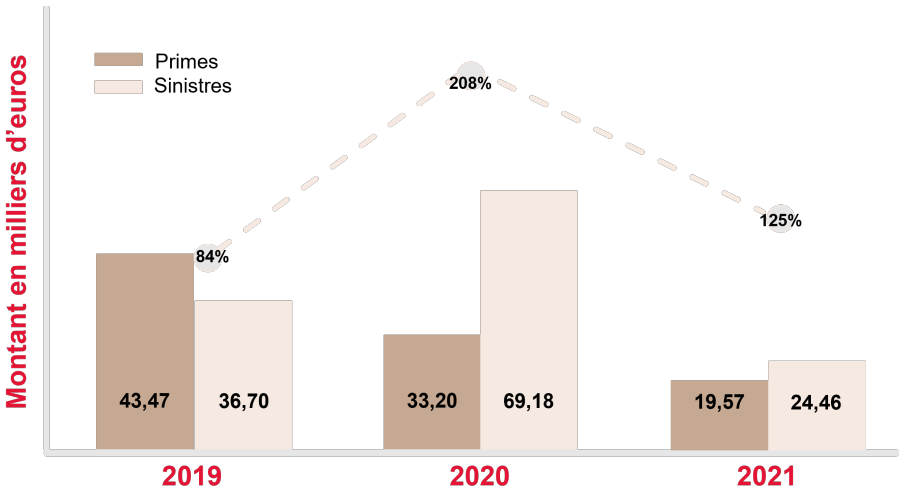

FIGURE 3.20 – S/P portefeuille sans les cryptovirus et malware

Exclure certaines attaques des garanties du contrat, notamment les cryptovirus ainsi que les *malware* viendraient détériorer les ratios combinés. Les cryptovirus constituent plus de la moitié du portefeuille (59%). Retirer ces dernières de l'analyse permettrait à la fois

d'améliorer le niveau d'indemnisation global de l'assureur car, selon la table 3.2, ce sont ces attaques qui coûtent le plus aux compagnies. Néanmoins, ne pas les assurer excluera du portefeuille plus de la moitié des entreprises, avec les primes y afférant. C'est pourquoi, d'après le graphe ci-dessus, le S/P 2020 se détériora de 30 points de pourcentages et de 35 points de pourcentages en 2021.

Et si nous proposions une méthode de tarification alternative ?

Une méthode alternative pourrait être proposée à l'aide d'une approche « classique ». Rappelons que lorsqu'un client souhaite souscrire à un nouveau contrat d'assurance, l'assureur doit déterminer la prime que l'assuré devra payer en fonction de certaines caractéristiques. Cette prime reflète le coût d'un assuré au cours d'une certaine période ; elle doit être à la fois suffisamment élevée pour que la compagnie d'assurance puisse prendre en charge un éventuel sinistre, dont le coût peut être élevé, subi par l'assuré et à la fois suffisamment basse pour que l'assuré accepte de signer le contrat et qu'il ne parte pas dans une autre compagnie d'assurance. Comme nous l'avons vu précédemment, le coût d'un assuré n'est pas connu au moment du calcul de la prime. Il faut donc utiliser des méthodes statistiques pour essayer d'estimer ce coût au mieux en s'appuyant sur certaines caractéristiques de l'assuré. Le but de la tarification a priori est donc de trouver un modèle statistique permettant d'estimer cette prime.

D'un point de vue statistique, estimer la prime revient à effectuer une régression d'une variable réponse Y, représentant le coût de l'assuré, sur un ensemble de variables explicatives X, représentant les caractéristiques de l'assuré. Dans les modèles de tarification a priori, les variables explicatives considérées seront toutes qualitatives (les variables quantitatives étant regroupées en classes).

Le principe de la régression est de modéliser $\mathbb{E}[Y|X]$ comme une fonction g des variables explicatives X, soit

$$\mathbb{E}[Y|X] = g(X).$$

La variable Y s'écrit alors

$$Y = g(X) + \epsilon,$$

où ϵ est un bruit aléatoire. Il représente l'écart entre Y et son espérance conditionnelle, soit l'erreur que nous commettons lorsque nous remplaçons Y par son espérance conditionnelle. Supposons que nous disposons d'un échantillon de taille n de $(p+1)$-uplets (X, Y), le but est donc de retrouver la fonction g.

En reprenant la même problématique que pour le modèle de Lotka-Volterra, nous souhaitons déterminer le montant de la prime pure que l'assuré devra payer en fonction des variables explicatives présentes dans la base de données qui caractérisent l'assuré. Dans cette étude, ce sont les variables CSP, Metier et CA (chiffre d'affaire) qui pourraient être utilisés dans la modélisation des GLM. L'étude porte à la fois sur la détermination du montant moyen des sinistres (utilisation de GLM de type gamma et inverse-gaussien car les coûts sont tous strictement positifs) ainsi que sur la fréquence de sinistralité (utilisation de GLM poisson et binomial).

3.5 Limites de l'étude

3.5.1 Limites liées aux données

Les données utilisées dans ce mémoire comportent plusieurs limites :

- Nous ne disposons que du nombre d'assurés sinistrés dans notre portefeuille. De ce fait, tous les résultats présentés comportent un certain biais car ils n'englobent pas l'effet de mutualisation qu'il est possible de retrouver avec les assurés non sinistrés présents dans le portefeuille ;
- Nous ne disposons pas explicitement du chiffre d'affaires des entreprises. Ce dernier a dû être reconstruit à l'aide d'une seconde base de données client ;
- Nous ne connaissons pas l'exposition de chaque entreprise ni d'informations permettant de la reconstruire. De ce fait, il est alors impossible d'effectuer une tarification classique de type coût-fréquence ;
- La fenêtre de temps que nous considérons est assez restreinte. De ce fait, il est difficilement possible de projeter nos résultats sur plusieurs années ;
- Nous n'avons aucun élément de comparaison (outre le rapport officiel de l'AMRAE). En effet, les rares données issues d'études ne fournissent pas les mêmes résultats ceci impactant la qualité de notre analyse.

3.5.2 Limites liées au modèle

La méthode présentée dans ce mémoire présente plusieurs limites que nous avons identifiées dans le chapitre 2 avec la base de données PRC à l'aide du modèle de Lotka - Volterra de base. Cependant, comme le modèle a évolué, de nouvelles limites sont apparues :

- En considérant un paramètre e constant au fil du temps, nous prenons en compte une croissance ou décroissance pérenne de la dynamique des populations. Cependant, cela implique également que l'indice de risque ne peut pas changer de monotonie sur une fenêtre d'observation future ;
- Le modèle ne se calibre pas sur la sinistralité observée : il faut préalablement utiliser une méthode de lissage afin de pouvoir déterminer les paramètres optimaux ;
- Le nombre de sinistres est dû simplement à l'indice de risque des entreprises et à aucun autre élément ;
- Tous les cyber-criminels travaillent ensemble et ne rentrent jamais en conflit.

3.5.3 Limites liées à la modélisation

Lorsque les paramètres ont été calibrés et que l'indice de risque a été construit, nous avons dû faire des hypothèses pour la suite de la modélisation engendrant une limite dans notre étude. Lors de la tarification, nous nous sommes rapprochés des chiffres de l'AMRAE, notamment le S/P de 2019 pour obtenir le taux i à appliquer sur notre portefeuille permettant d'avoir le même niveau de ratio combiné. Cependant, l'AMRAE a construit cette étude avec tous les assurés contrairement à nous ou nous ne disposions seulement des assurés sinistrés.

3.6 Mise à jour de l'étude de l'AMRAE

L'AMRAE a publié sa deuxième étude annuelle de l'assurance du cyber risque en France (après réalisation de l'étude de tarification) : l'enquête LUCY édition 2022 [8]. Nous disposons à présent d'une année d'historique supplémentaire par rapport à l'étude de l'an dernier pour comprendre le risque cyber. Certaines modifications sont toutefois à noter concernant ce nouveau rapport comme les collectivités publiques qui n'ont pas été prises en compte en 2021 car leur faible recours au courtage ne permet pas d'obtenir des résultats pertinents. Notons que toute la rédaction du mémoire s'est construite en se basant sur l'édition 2021. Mais, au vu des résultats parus dans l'édition 2022, ces derniers ne viennent pas altérer les choix que nous avions pu opérer précédemment.

Selon Philippe Cotelle, après une année 2020 fortement déficitaire pour les assureurs sur le marché du risque cyber, ces derniers ont durci drastiquement les conditions de souscription avec notamment un doublement des primes, une réduction des garanties ainsi qu'une instauration de franchises importantes. De ce fait, le marché cyber se retrouve tendu car selon l'enquête LUCY, 11 des 251 grandes entreprises qui avaient souscrit une garantie cyber en 2020 ont préféré renoncer en 2021.

Les résultats de l'étude ont été produit, comme pour la version 2021, grâce à plusieurs courtiers spécialistes du risque d'entreprise. Ils avaient à répondre à un questionnaire portant à la fois sur la couverture du risque cyber (nombre d'entreprises ayant souscrit une police cyber, couverture souscrite, montant de la prime brute) ainsi que sur les sinistres indemnisés (nombre de sinistres, élément déclencheur, nature de l'impact, montant de l'indemnisation).

Selon l'AMRAE, après une année 2020 (crise sanitaire) déficitaire, le marché de l'assurance cyber est redevenu « équilibré » avec un ratio sinistres à primes technique de 88% pour l'ensemble des entreprises.

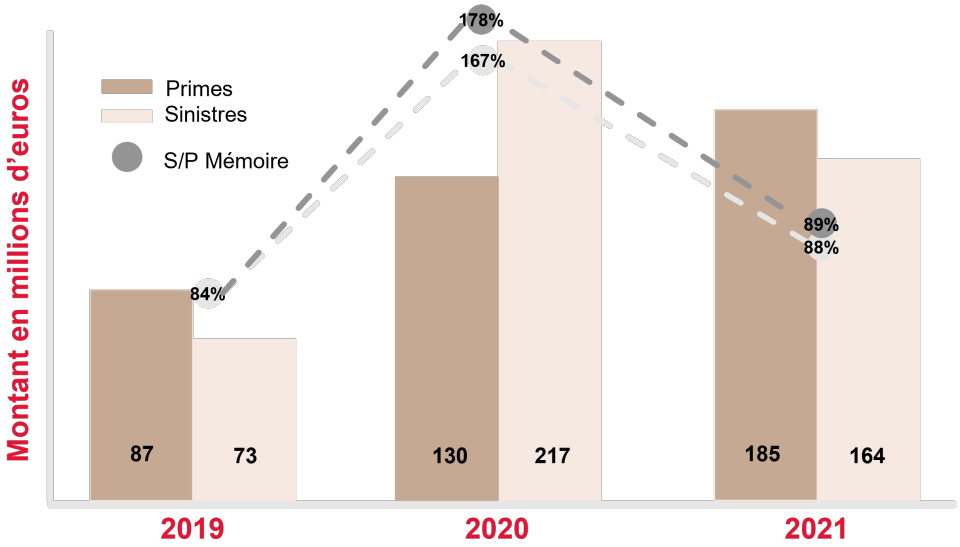

FIGURE 3.21 – Résultats techniques des assureurs

Ce phénomène peut s'expliquer de part la très forte augmentation du volume global de primes encaissées par les assureurs (environ 48% en 2021) alors que les capacités souscrites

ont diminué de 21%. De plus, nous avons également assisté à la mise en place de franchises très élevées pouvant aller jusqu'à 4 millions d'euros pour les grandes entreprises. La question qui se pose dans cet article est la suivante : les entreprises doivent-elles toujours s'assurer ? Selon l'enquête LUCY menée par l'AMRAE et à l'aide du tableau ci-dessous, il est constaté que les taux de couverture sont en baisses.

TABLE 3.8 – Évolution des taux de couverture

		Entreprises assurées				
Taille	Effectif total 2021	en 2019	en 2020	en 2021	Croissance 2021/2020	Taux de couverture 2021
GE	287	207	251	240	-4,4%	84%
ETI	5 763	307	441	530	20,2%	9%
PME	139 971	311	362	322	-11%	0,2%
TPE	3 723 742	7 641	7 670	10 936	5,4%	0,2%

Comme nous l'avons vu dans le premier chapitre, la volatilité des sinistres cyber engendre, toute chose égale par ailleurs, une forte variation des S/P. En effet, en prenant l'exemple de 2019, aucun sinistre de très forte sévérité (entre 10 et 40 millions d'euros) n'aurait été déclaré par les grandes entreprises. Mais en 2020 4 sinistres l'auraient été ainsi que 6 en 2021. Cette fluctuation engendre donc une variation importante du ratio sinistres à primes passant de 44% en 2019 à plus de 190% en 2020 pour ensuite revenir à 58% en 2021 pour les grandes entreprises. Comme précisé dans l'enquête LUCY de 2021 et à l'aide du graphique ci-dessous, il est possible d'observer une certaine stabilité pour les sinistres de faible, moyenne et grande sévérités entre les 3 années d'historique mais une instabilité pour les sinistres de très forte sévérités. Cependant, ces chiffres ne sont pas à prendre mot comptant car nous ne disposons encore une fois que de 3 années d'historique.

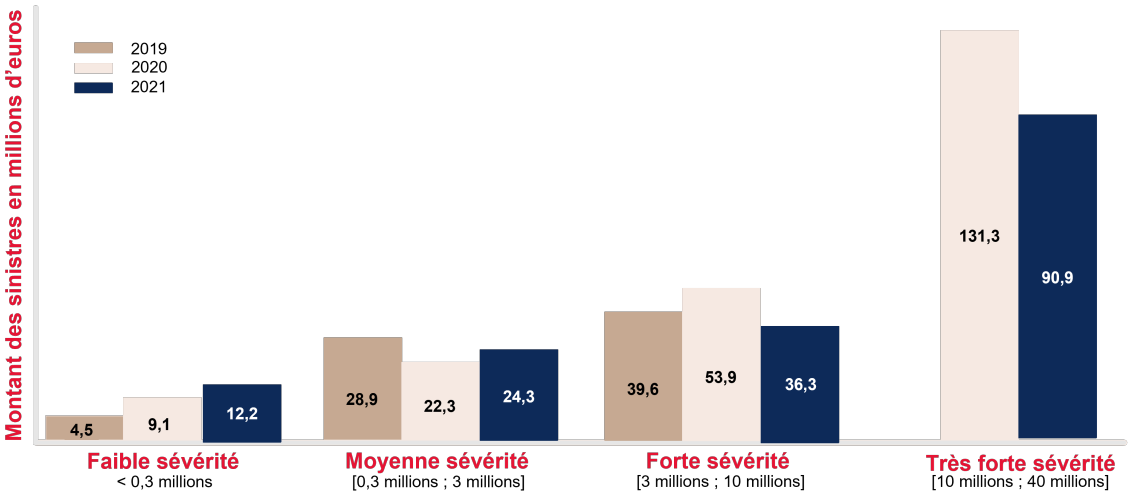

FIGURE 3.22 – Comparaison des sinistres entre 2019 et 2021 selon le degré de sévérité d'après l'étude LUCY de 2022

Les conclusions de l'AMRAE seraient plus positive que lors du rapport précédent. En effet, après avoir augmenté les taux de primes, les franchises ainsi que réduit les capacités, le marché de l'assurance cyber est redevenu « rentable » avec des résultats semblable à ceux

de l'année 2019. Cependant, cela c'est fait au détriment de certaines entreprises qui, au vu des changements drastiques, ont décidé de ne plus s'assurer. Le rapport évoque également que l'assurance classique ne permet pas de couvrir ce risque et ouvre sur des perspectives que nous avons abordé dans ce mémoire comme par exemple l'utilisation de mécanismes d'amortissement spécifiques pour les « catastrophes cyber » qui pourrait ressembler à ce que nous connaissons sur le modèle du régime *CatNat*. La tarification que nous avons proposé dans les sections précédentes pourraient donc être considérées comme pertinente au vu du discours qu'envisage l'AMRAE. Avec cette méthode, et sans avoir de référentiel sur 2021 (car le mémoire est bien basé sur l'enquête LUCY de 2021 et non 2022), nous avons obtenu un S/P en 2021 de 89% contre 88% dans le rapport de l'AMRAE.

Conclusion

Le risque cyber est aujourd'hui un enjeu pour les assureurs. Ces derniers essaient au mieux de les cerner et de proposer des contrats afin d'assurer les évènements y afférant.

Ce mémoire avait pour objectif de proposer une modélisation du risque cyber qui pourrait, par la suite, être utilisée pour de la tarification individuelle ou collective.

Pour ce faire, nous avons choisi d'utiliser le modèle de Lotka-Volterra. Par manque de données, nous avons pris plusieurs hypothèses en nous basant sur des indications trouvées dans la littérature, et notamment l'étude LUCY de l'AMRAE (version 2021). C'est pourquoi, il convient de rester prudent lors de l'analyse des résultats.

Ce modèle a permis, dans un premier temps, de construire un indice de risque cyber à travers le temps en utilisant pour simple variable endogène le nombre de sinistres survenus. Afin de calibrer les paramètres du modèle, il a fallu utiliser un lissage de Whittaker-Henderson sur le nombre de sinistres.

Une fois le lissage opéré, la calibration des paramètres a pu être effectuée. Pour cela, le choix retenu a été de minimiser la somme des écarts quadratiques entre la courbe générée par des paramètres initiaux et celle retraçant la sinistralité. Lorsque le modèle a déterminé la dynamique du nombre de sinistres (prédateurs), l'indice de risque a pu être déterminé (proies).

Tous les paramètres nécessaires à la tarification étaient disponibles. Contrairement à une approche classique de type fréquence-sévérité, nous nous sommes rapproché de ce qui est utilisé dans le régime *CatNat* afin d'implémenter une méthode de tarification alternative.

Cette méthode bien mise en place, nous nous sommes alors intéressés au niveau des S/P lorsque nous faisions varier nos hypothèses. Nous avons ainsi pu mettre en évidence que certains changements d'hypothèse ne seraient que peu significatifs sur notre portefeuille (hypothèse sur le paramètre de lissage, hypothèse sur l'indice de risque). Nous nous sommes également interrogés sur la façon d'apporter une réponse optimale à la question de la cible et du contenu du contrat cyber en cherchant à mesurer l'impact de certaines exclusions (chiffre d'affaire des entreprises inférieures à 1 millions, collectivités et associations, cryptovirus et *malware*) sur le S/P.

Il reste bien évidemment de nombreux travaux à effectuer. Nous pourrions par exemple chercher à creuser encore un peu le sujet en améliorant la prise en compte de l'indice de risque dans la détermination de la prime pure ou encore moduler la formule de cette dernière afin de mieux appréhender le taux de prélèvement du chiffre d'affaire.

Par ailleurs, une autre question nous intéresse. Nous avons présenté un modèle alternatif

de Lotka-Volterra, que nous avons sélectionné. Cependant, il serait également intéressant de modifier ces équations en rajoutant par exemple une troisième population et de regarder l'impact de ces changements sur notre tarification.

Bibliographie

[1] Acronis [2014], 'The nhs cyber attack', *Acronis* .

[2] ANSSI [2021], 'Etat de la menace rançongiciel'.

[3] APREF [2016], 'Etude sur les « cyber risques » et leur (ré)assurabilité'.

[4] Avast [2020], 'Qu'est-ce que wannacry ?', *Avast* .

[5] CARF [2021], 'Cartographie prospective 2021'.

[6] CESIN [2022], 'Baromètre de la cybersécurité des entreprises'.

[7] Cotelle, P. [2021], 'Lucy : Lumière sur la cyberassurance'.

[8] Cotelle, P. [2022], 'Lucy : Lumière sur la cyberassurance'.

[9] Eling, M. and Loperfido, N. [2017], 'Data breaches : Goodness of fit, pricing and risk measurement', *Insurance : Mathematics and Economics* .

[10] Faure-Muntian, V. [2021], 'La cyber-assurance'.

[11] Hillairet, C., Boumezoued, A. and Bessy-Roland, Y. [2020], 'Multivariate hawkes process for cyber risk insurance'.

[12] Jacobs, J. [2014], 'Analyzing ponemon cost of data breach', *datadrivensecurity* .

[13] Khan, N. A., Brohi, S. N. and Zaman, N. [2020], 'Ten deadly cyber security threats amid covid-19 pandemic'.

[14] Lopez, O. and Hillairet, C. [2020], 'Propagation of cyber incidents in an insurance portfolio : counting processes combined with compartmental epidemiological models'.

[15] Lopez, O., Thomas, M. and Farkas, S. [2020], 'Cyber claims analysis through generalized pareto regression trees with applications to insurance pricing and reserving'.

[16] Lustman, F. [2022], 'Bâtir une économie de la donnée innovante et protectrice en faveur des français'.

[17] Powel, D. and STrou, R. [2003], 'Conceptual model and architecture of maftia', *MAFTIA* .

[18] Research, P. I. [2021], 'Trend micro index on the state of cybersecurity'.

[19] Vache-Marconato, G. [2010], 'Evaluation quantitative de la sécurité informatique : approche par les vulnérabilités'.

Liste des tableaux

Table des figures