Mémoire présenté devant l'Université de Paris-Dauphine
pour l'obtention du Certificat d'Actuaire de Paris-Dauphine
et l'admission à l'Institut des Actuaires
le

Par : Guillaume RIGAUD
Titre : Modèle d'accumulation du risque cyber

Confidentialité : ☐ NON ☑ OUI (Durée : ☐ 1 an ☑ 2 ans)

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

Membres présents du jury de l'Institut des Actuaires

Entreprise : AXA GRM
Nom :
Signature :

Membres présents du jury du Master Actuariat de Paris Dauphine

Directeur de mémoire en entreprise :
Nom : Xavier SERVEL
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 :

Signature du responsable entreprise

Bibliothèque :

Signature du candidat

Remerciements

Un mémoire n'est pas la réalisation d'un seul individu. C'est le reflet d'une formation académique et le fruit de discussions et échanges permettant l'aboutissement d'un projet. Pour cela, je souhaite remercier toutes les personnes qui ont permis la réalisation de ce mémoire :

- Monsieur Xavier SERVEL, pour l'encadrement qu'il m'a prodigué tout au long de mon stage, m'accordant sa confiance et m'apportant toute son expertise pour mener à bien ces travaux

- Monsieur Julien STOEHR, pour ses précieux conseils sur les méthodes bayésiennes, son attention à l'égard de mes travaux et sa grande disponibilité

- Monsieur Pierre CARDALIAGUET, pour ses précieuses relectures et ses recommandations avisées

- l'équipe P&C Actuarial and Business Review d'AXA Group Risk Management, qui m'a chaleureusement accueilli et a, au cours de nombreuses discussions, contribué à l'enrichissement de ce mémoire

- l'ensemble des enseignants chercheurs du CEREMADE, pour leur disponibilité et bienveillance et surtout pour la qualité des cours dispensés tout au long de ces 5 années passées à l'Université Paris Dauphine

- mes amis, qui ont rendus inoubliables ces années d'études

- ma famille, pour son soutien permanent.

Résumé

Le risque cyber constitue un défi pour la gestion des risques. Les (ré)assureurs redoutent principalement une accumulation de sinistres provoqués par un même évènement ou attaque cyber. La quantité et la qualité des données relatives à des évènements cyber limitent l'application de modèles actuariels classiques pour modéliser ce risque. Pour évaluer l'impact d'une telle catastrophe, il est préférable pour l'assureur de procéder à une approche par scénario. L'objectif principal de ce mémoire est la mise en place d'un nouveau scénario d'accumulation à intégrer au modèle interne cyber du groupe AXA. Nous parlerons d'évènement d'accumulation lorsqu'un même évènement ou attaque cyber touche au moins deux polices d'assurance distinctes.

La première partie de ce mémoire permet d'établir le contexte de l'étude. Une définition du risque cyber est proposée et à travers des exemples concrets, nous déduisons les principales spécificités du risque cyber. Le cadre réglementaire est aussi dressé et son influence sur le marché de l'assurance cyber est établie. Le marché de l'assurance cyber est ensuite présenté avec ses principales garanties et perspectives de croissance. La question de l'assurabilité est posée, tout en proposant des pistes pour appréhender au mieux ce risque. Nous dressons enfin le cadre spécifique de notre étude et décrivons les données à notre disposition.

Dans une seconde partie, nous présentons la structure du modèle cyber avant d'introduire le scénario existant qui repose sur une attaque de serveur cloud. Nous montrons une utilisation du modèle en y intégrant un portefeuille de coassurance dont certaines variables sont manquantes. Nous expliquons notre démarche pour simuler ces variables ou en obtenir un proxy et évaluons nos ajustements. Nous nous intéressons ensuite à l'étude CyRim 2019 décrivant une attaque ransomware. Nous expliquons nos ajustements et hypothèses faites pour implémenter ce scénario avant de l'utiliser à titre de comparaison avec le scénario cloud.

Pour prendre en compte une plus grande diversité de menaces cyber, il est nécessaire d'incorporer plusieurs scénarios au modèle interne cyber *affirmative First Party*. NotPetya est à l'heure actuelle le ransomware le plus dévastateur : nous étudions donc cet évènement avant d'introduire la modélisation d'un scénario ransomware qui sera ajouté au scénario cloud. C'est l'objet de notre troisième et dernière partie. Pour modéliser ce second scénario nous effectuons une analogie entre le risque pandémique et le risque cyber. Nous présentons d'abord différents modèles épidémiologiques compartimentaux et choisissons d'adapter le modèle SIR au risque cyber. Nous décrivons la structure du modèle SIR adapté et dressons les obstacles à priori d'une telle analogie. Nous utilisons le cadre bayésien pour mettre à profit nos connaissances acquises sur NotPetya et répondre à l'absence de données complètement observées. Nous nous donnons ensuite 3 jeux de lois *a priori* pour nos paramètres induisant 3 modèles statistiques différents. Nous nous intéressons aux lois *a posteriori* obtenues pour chacun de ces modèles à l'aide de la méthode ABC (Approximate Bayesian Computation). Nous choisissons ensuite un modèle que nous utilisons pour obtenir la distribution de la perte assurée. Les avantages et inconvénients de notre approche sont établis avant de proposer des pistes d'amélioration.

Mots clés : risque cyber, risque systémique, modèle d'accumulation, pandémie, vol de données, ransomware, cloud, virus, méthode ABC

Abstract

Cyber risk is a challenge when it comes to risk management. (Re)insurers mainly fear an accumulation of claims caused by the same event or cyber-attack. The quantity and quality of data relating to cyber events limits the application of traditional actuarial models to model this risk. To assess the impact of such a disaster, it is preferable for the insurer to use a scenario-based approach. The main objective of this dissertation is to set up a new accumulation scenario to be added into AXA Group's cyber internal model. We will speak of an accumulation event when the same event or cyber-attack affects at least two separate insurance policies.

The first part of this dissertation sets the context of our study. A definition of cyber risk is proposed and through concrete examples we infer the main characteristics of cyber risk. The regulatory environment is also presented, with its influence on cyber insurance market. The cyber insurance market is introduced with its main covers and growing perspectives. The question of insurability is raised, while proposing solutions to better measure cyber risk. We finally outline the specific context of our study and present the available data.

In the second part, we are explaining the structure of the cyber model before introducing its existing scenario based on a cloud server attack. We use the model in which we integrate a portfolio with missing variables. We explain our strategy to generate those missing variables or obtain proxies and evaluate our adjustments. Then, we focus on the ransomware attack from the 219 CyRim study. We explain our adjustments and hypothesis made to implement the scenario and use it to compare the order of magnitude of insurance losses with the one from the cloud scenario.

To take into account a broader array of cyber threats, it is necessary to integrate multiple scenarios in the cyber affirmative First Party internal model. At this time, NotPetya is the most devastating ransomware: we studied this event before presenting the ransomware scenario modeling which will be added to the cloud scenario. This is the purpose of our third and last part. To model this ransomware scenario, we draw the parallel between pandemic risk and cyber risk. We first introduce some compartmental epidemiological models and choose to adapt the SIR model to cyber risk. We describe the structure of the adapted SIR model and outline the obstacles stemming from this approach. We use the Bayesian framework to take advantage of the knowledge from NotPetya and estimate the law of parameters on partially observed and fragmented data. We use three sets of prior laws deriving three different statistical models and estimate the posterior law of parameters for each of these models with the Approximate Bayesian Computation method. Then, we choose a model which we use to simulate the insured loss and get the loss distribution. Finally, the advantages and drawbacks of our approach are established and we suggest some complementary work and improvements.

Key words : cyber risk, systemic risk, accumulation model, pandemic, data breach, ransomware, cloud, malware, ABC method

Note de Synthèse

Contexte d'étude et problématique

Le risque cyber regroupe des atteintes faites tant aux données qu'aux systèmes électroniques résultant d'un acte volontaire ou involontaire ayant pour conséquence tout type de dégâts. Cette définition regroupe un très large panel d'évènements. Les (ré)assureurs craignent principalement une accumulation de sinistres provoqués par un même évènement ou attaque cyber. Un évènement d'une telle ampleur est difficile à évaluer en raison du faible nombre de données disponibles et de nombreuses incertitudes quant à la forme que pourrait prendre la prochaine attaque cyber mondiale.
Les phénomènes d'accumulation vont à l'encontre de la mutualisation des risques, qui est un principe primordial de l'assurance. Une modélisation classique supposant l'indépendance entre la fréquence et la sévérité est donc à proscrire pour modéliser des évènements d'accumulation. Pour évaluer l'impact qu'aurait une catastrophe cyber sur son portefeuille, il est préférable pour l'assureur de procéder à une approche par scénario.

Ce mémoire se focalise essentiellement sur la gestion des risques liés aux garanties cyber dites *affirmative First Party*, c'est-à-dire les garanties couvrant explicitement le risque cyber pour des dommages matériels et immatériels subis par l'assuré. Notre objectif principal est la construction d'un scénario d'accumulation pouvant être incorporé au modèle cyber *affirmative First Party* du groupe AXA.

Étude du risque cyber

Avant de construire notre scénario, il est important d'établir les caractéristiques du risque cyber. Le caractère évolutif du risque cyber pousse les assureurs à adapter les contrats qu'ils proposent et à suivre l'évolution des types de garanties vendues pour estimer au mieux leurs risques. L'évolution du type d'attaques et évènements probables est aussi à prendre en compte dans la modélisation du risque. Le caractère systémique et contagieux du risque cyber suggère une portée plus importante que tous les autres risques : les frontières géographiques sont quasi inexistantes pour un tel risque. Le caractère imprévisible du risque force les assureurs à considérer tous les scénarios possibles afin d'immobiliser un niveau de capital suffisant pour honorer leurs engagements.
Le risque cyber étant un risque nouveau, les bases de sinistres des assureurs disposent d'un faible historique. Par conséquent, l'assureur n'est pas en mesure de construire ses modèles à partir de sa propre expérience acquise à travers les sinistres survenus sur son portefeuille. Les sinistres d'un portefeuille sont en effet peu représentatifs du risque cyber. Pour compléter ses bases et renforcer ses connaissances, l'assureur peut recourir à des bases de données externes recensant des évènements cyber. Ces bases comportent souvent des biais sectoriels et géographiques auxquels s'ajoute un biais temporel provenant de l'évolution de la réglementation en matière d'obligation de notifier en cas de *data breach*. L'utilisation de ces bases de données externes soulève donc des questions de fiabilité mais aussi d'absence d'exposition au risque. Ces bases sont difficilement utilisables telles quelles pour construire tout un modèle avec une approche fréquence/sévérité. Elles peuvent néanmoins servir à vérifier certaines hypothèses ou conjectures utilisées dans les modèles de l'assureur.

Modèles existants

Pour mieux comprendre les enjeux liés à l'approche par scénario, nous présentons la structure du modèle cyber actuel et le scénario dont il est muni : une attaque de serveur cloud. Nous nous familiarisons avec le modèle en y incorporant un portefeuille de coassurance. A travers cet exercice, nous nous sensibilisons à l'importance de la qualité des données lors de l'évaluation du risque. Pour le risque cyber, la problématique des données est centrale : elle va de la gestion interne des données relatives aux contrats d'assurance, aux conditions d'utilisation de bases externes. L'implémentation de l'attaque « Bashe » issue de l'étude CyRim nous permet de découvrir d'autres méthodes de construction d'un scénario d'accumulation. La perte bicentenaire renvoyée par l'attaque Bashe n'est pas identique à celle renvoyée par le scénario cloud, mais l'ordre de grandeur est tout de même comparable, ce qui conforte donc les choix faits pour la construction du scénario cloud. Nous notons donc que la répartition des sous-couvertures de notre portefeuille et le choix des sous-couvertures impactées par le scénario influent sur la perte assurée. Ces éléments motivent la mise en place d'un scénario supplémentaire pour compléter notre vision du risque porté par notre portefeuille.

Construction d'un scénario d'accumulation : le ransomware

Un modèle doté d'un seul scénario a tendance à toucher toujours les mêmes garanties, ce qui ne signifie pas pour autant que les autres garanties ne comportent aucun risque, leur risque n'est simplement pas modélisé par le scénario en question. Le recours à un catalogue de scénarios permet donc à l'assureur d'avoir une vision plus générale du risque porté par son portefeuille.
Nous souhaitons que notre modèle puisse reproduire des attaques similaires au ransomware NotPetya, et qu'il permette aussi d'étudier les conséquences de NotPetya dans des conditions plus adverses, par exemple si l'attaque avait duré plus longtemps ou que la rançon avait été plus élevée.

Le risque cyber est souvent comparé au risque de pandémie. Ces deux risques ont notamment en commun leur caractère contagieux, systémique et imprévisible. Nous décidons d'exploiter cette analogie pour construire notre scénario ransomware et adaptons un modèle épidémiologique pour modéliser la propagation d'un ransomware. Nous avons choisi d'incorporer un SIR adapté à notre problème pour générer des victimes munies de leurs temps infectieux, de réparation et sévérités individuelles. Chaque attaque simulée est donc la réalisation z d'une variable aléatoire que nous notons Z. Une fois ces victimes générées, un coût économique réparti en garanties leur est associé.
Ce coût économique est obtenu au moyen d'une fonction h que nous avons construite en nous appuyant sur des données récoltées sur NotPetya.

Estimation des paramètres du modèle

Pour estimer les paramètres de notre SIR adapté, nous devons utiliser une méthode permettant de tirer parti des données parcellaires récoltées sur NotPetya.
Pour NotPetya, les valeurs des hyper-paramètres du modèle sont connues (durée de l'attaque, système attaqué, coût de la rançon) et sont donc fixées pour procéder à l'estimation des paramètres du modèle. Nous choisissons le cadre bayésien permettant de mettre à profit nos connaissances acquises sur NotPetya et d'incorporer une notion d'incertitude sur ces paramètres via l'estimation de la loi *a posteriori* de ces derniers. Nous écartons l'utilisation de la méthode MCMC (Markov Chain Monte Carlo) pour estimer la loi *a posteriori* des paramètres, puisqu'elle requiert la connaissance de la

vraisemblance du modèle à une constante multiplicative près. Dans notre cas, la vraisemblance est difficilement exprimable puisqu'elle dépend d'un espace de grande dimension. Nous avons recours à la méthode ABC (Approximate Bayesian Computation) pour contourner ce problème. ABC est une méthode d'acceptation rejet nous permettant de passer outre le calcul de la vraisemblance du modèle : les points acceptés par l'algorithme sont ceux situés dans une boule proche d'une transformation statistique de notre observation réelle (appelée cible): NotPetya. Cette transformation statistique de nos observations n'est autre que le nombre de victimes normalisé et le coût total de l'évènement normalisé. Cette transformation $\eta(Z)$ fait intervenir notre fonction de coût h, ce qui permet de mettre à profit toutes nos connaissances acquises *a priori*.
Les données récoltées sur NotPetya étant très parcellaires, le recours à cette transformation statistique nous permet de comparer des observations synthétiques issues du modèle à notre observation réelle, et ainsi d'estimer la loi *a posteriori* des paramètres du modèle dans un voisinage de notre cible.

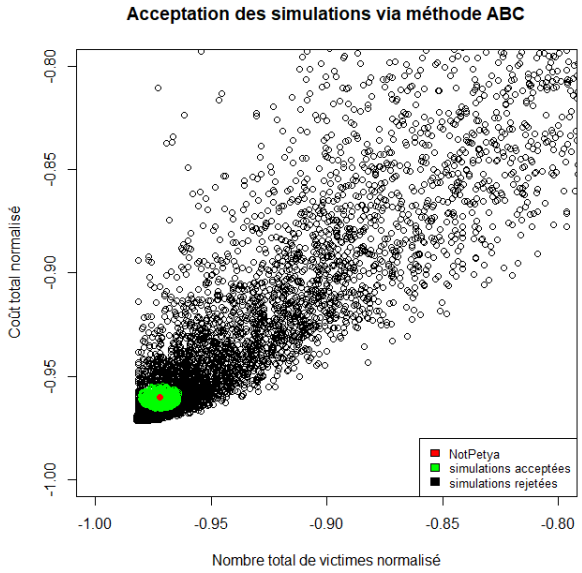


Figure 1 - Zone d'acceptation de la méthode ABC (modèle 1)

Nous nous donnons trois jeux de lois *a priori* induisant 3 modèles statistiques différents. Les comportements des modèles estimés sont étudiés et nous choisissons finalement le troisième modèle, permettant de reproduire NotPetya mais aussi tous les évènements reliant NotPetya à WannaCry (figure 2). Notre modèle est donc en mesure de générer trois types d'évènements : des évènements de forte sévérité individuelle et de 'faible' portée (NotPetya), des évènements de moins grande sévérité individuelle et de plus grande portée (WannaCry), ou bien des évènements centraux nouveaux mais jugés vraisemblables puisqu'ils se situent entre NotPetya et WannaCry.

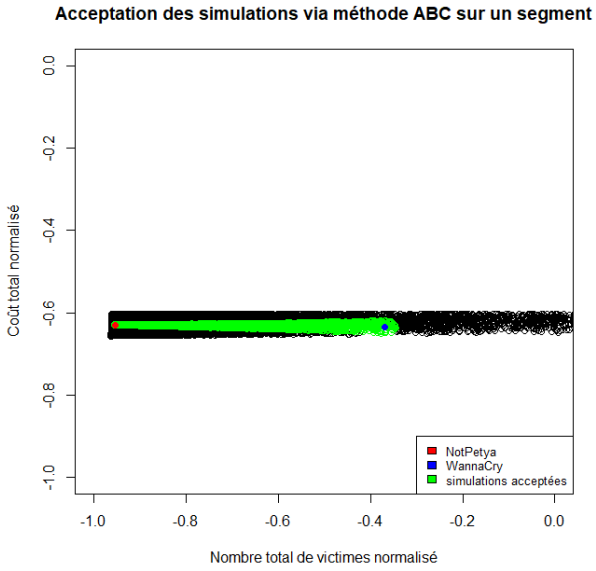


Figure 2 - Zone d'acceptation autour du segment reliant NotPetya à WannaCry (modèle 3)

Nous procédons par bootstrap sur les paramètres acceptés par ABC pour simuler le modèle suivant la loi *a posteriori*. Pour procéder aux simulations, nous rendons aléatoires les hyper-paramètres fixés pour l'estimation et analysons l'impact de chacun de ces hyper-paramètres sur nos simulations. Les simulations ainsi réalisées permettent de répondre à la question suivante : « Qu'aurait-il pu se passer si les virus NotPetya, WannaCry ou un compromis entre les deux avaient visé un autre système d'exploitation, que le coût de la rançon avait été plus élevé et que l'attaque n'ait pas été endiguée si vite ? ».
Ce modèle ne permet pas de répliquer ni de prévoir le comportement de n'importe quel type de ransomware sur notre portefeuille. En revanche, il permet de simuler des variantes proches de NotPetya ou WannaCry dans des conditions plus adverses, pouvant être qualifiées de scénarios catastrophe.

Nous étudions ces évènements générés et calculons le quantile à 99.5% de la perte assurée à l'échelle du groupe AXA et de chacune de ses entités. Nous expliquons aussi comment ce scénario pourrait être intégré au modèle interne cyber du groupe AXA.

Avantages, limites et travaux futurs

Enfin, nous dressons les avantages et inconvénients du modèle et proposons des pistes d'amélioration.
Le modèle présenté répond à nos objectifs initiaux dans la mesure où il complète la vision du risque porté par le portefeuille AXA sur les contrats cyber *affirmative First Party*. Il utilise des variables différentes du scénario cloud pour affecter une notion de risque aux entreprises assurées ce qui contribue à diversifier la vision du risque porté par les assurés.
La construction du modèle et la méthode d'estimation ont su tirer profit de la faible quantité de données disponibles tout en gardant un esprit cohérent. La méthode d'estimation pourra être reconduite si de nouveaux évènements ont lieu ou si un évènement fictif représentant les craintes futures voulait être pris en compte.
En revanche, il faut garder à l'esprit que le modèle n'est pas doté d'une grande précision puisque nous avons recours à de nombreux proxies pour approximer certaines variables non présentes dans nos bases de données mais utilisées par le modèle. De plus, nous déconseillons l'utilisation de la méthode d'estimation employée pour des portefeuilles plus petits. En effet, la méthode d'estimation s'effectue

conditionnellement aux entreprises présentes dans le portefeuille AXA. Ce dernier étant suffisamment grand et diversifié, il représente relativement bien l'économie mondiale. En revanche pour des plus petits portefeuilles ou des portefeuilles non diversifiés, la méthode ne permettrait pas de reproduire des évènements comme NotPetya ou WannaCry. Les attaques cyber étant souvent fulgurantes, l'utilisation classique d'un modèle épidémiologique visant à anticiper la progression d'un virus pour mieux le stopper est difficile ici, mais peut tout de même être mise en œuvre par l'assureur pour tenter d'évaluer une borne supérieure de sa perte en cas de nouveau ransomware.

Nous avons étudié l'impact des paramètres et variables du modèle via une matrice de corrélation et des graphiques. Il serait intéressant de procéder à des tests de sensibilité plus poussés. Au vu de la structure de la fonction de coût économique, nous anticipons une forte sensibilité positive du modèle au chiffre d'affaire des assurés, variable à laquelle le modèle cloud était très peu sensible. Le modèle pourra être enrichi d'informations plus précises sur les assurés pour éviter le recours aux proxies. Il sera alors intéressant d'étudier l'évolution des résultats. La structure du modèle laisse aussi la possibilité d'incorporer des scores de risque sur les assurés lorsqu'ils seront disponibles.

Synthesis Note

Study context and issues raised

Cyber risk can be defined as breaches or attacks on both data and electronic systems resulting from a voluntary or involuntary act causing any type of damage. This definition encompasses a very wide range of events. (Re)Insurers mainly fear an accumulation of claims caused by the same event or cyber-attack. An event of this magnitude is difficult to assess because of the small amount of data available and many uncertainties regarding the shape of the next global cyber-attack.
The phenomena of accumulation go against the pooling of risks, which is a fundamental principle of insurance. A standard modeling assuming the independence between the frequency and the severity has to be avoided to model such events of accumulation. To evaluate the impact of a cyber disaster on his portfolio, the best course of action for an insurer is to rely on a scenario based approach.

This dissertation primarily focuses on the risk management of risks related so-called affirmative First Party cyber covers, which are contracts explicitly covering cyber risk for both material and immaterial damages suffered by the insured. Our main objective is the construction of an accumulation scenario which can be incorporated into the AXA Group's affirmative First Party cyber model.

Study of cyber risk

Before building our scenario, it is important to establish the characteristics of cyber risk. The evolving nature of cyber risk encourages insurers to adapt the contracts they offer and to monitor the evolution of the types of cover sold in order to best estimate their risks. The evolution of the type of attacks and probable events has also to be taken into account in risk modelling. The systemic and contagious nature of cyber risk suggests a greater scope compared all other risks: geographical borders are almost non-existent for such a risk. The unpredictability of the risk forces insurers to consider all possible scenarios in order to allocate a sufficient level of capital to comply with their obligations.
Since cyber risk is a new risk, insurers' claims databases have a short history. As a result, the insurer is not in a position to build his models from his own experience gained through claims on its portfolio. Claims in a portfolio are not very representative of the cyber risk. To complete their databases and strengthen their knowledge, insurers can use external databases listing cyber events. These databases often include sectoral and geographical biases, as well as a time bias resulting from changes in the regulations regarding the obligation to notify the regulator in the event of a data breach. The use of these external databases therefore raises questions of reliability and the absence of exposure to risk. These databases are difficult to use to build a whole model with a frequency severity approach. However, they can be used to test certain assumptions or conjectures used in the insurer's internal model.

Existing models

To better understand the issues related to a scenario based approach, we present the structure of the current cyber internal model and the scenario associated: a cloud server attack. We familiarize ourselves

with the model by incorporating a coinsurance portfolio. Through this exercise, we have built some awareness about the importance of data quality when assessing risk. For cyber risk, the data issue is key: it ranges from the internal management of data related to insurance contracts to how external databases are used. The bicentenary loss returned by the Bashe attack is not identical to the one returned by the cloud scenario, but the order of magnitude is still comparable, which therefore supports the choices made for the construction of the cloud scenario. We therefore note that the distribution of covers in our portfolio and the choice of covers impacted by the scenario influence the insured loss. These elements motivate the implementation of an additional scenario to complete our vision of the risk carried by our portfolio.

Building an accumulation scenario: ransomware

A model based on only one scenario tends to always impact the same covers, which does not mean that the other coverages do not carry any risk, their risk is simply not modelled by the scenario implemented. The use of a catalogue of scenarios therefore allows the insurer to have a more general view of the risk carried by his portfolio.
We want our model to be able to reproduce attacks similar to the NotPetya ransomware and expect that it would also allow us to study the consequences of NotPetya in more adverse conditions, for example, if the attack had lasted longer or the ransom price had been higher.
Cyber risk is often compared to pandemic risk. These two risks have in common, in particular, their contagious, systemic and unpredictable nature. We have decided to use this analogy to build our ransomware scenario and adapt a compartmental epidemiological model to simulate the spread of a ransomware. We have chosen to incorporate a well-adapted SIR to our problem to generate victims with their infectious times, reparation and individual severity. Each simulated attack is therefore a realization z of a random variable that we note Z. Once these victims are generated, they are associated with an economic cost divided into guarantees. This economic cost is obtained by means of a function h that we have constructed based on data collected on NotPetya.

Estimation of model parameters

To estimate the parameters of our adapted SIR, we have to use a method which takes advantage of the fragmented data collected on NotPetya.
For NotPetya, the values of the model's hyperparameters are known (duration of the attack, system attacked, cost of the ransom) and are therefore fixed to estimate the model parameters. We choose the Bayesian framework to leverage the knowledge from NotPetya and incorporate a notion of uncertainty on these parameters through the estimation of their *posterior* law. We discard the use of the MCMC (Markov Chain Monte Carlo) method to estimate the *posterior* law of the parameters, since it requires knowledge of the model's likelihood within a multiplicative constant. In our case, the likelihood is difficult to express since it depends on a large space. We use the ABC (Approximate Bayesian Computation) method to work around this problem. ABC is a rejection acceptance method allowing us to bypass the calculation of the model's likelihood: the points accepted by the algorithm are those located in a ball around a statistical transformation of our real observation (called target): NotPetya. This statistical transformation of our observations is the normalized number of victims and the normalized total cost of the event. This transformation $\eta(Z)$ involves our cost function h, which allows us to take advantage of our *prior* knowledge acquired on NotPetya.

Since the data collected on NotPetya is very fragmented, the use of this statistical transformation enables us to compare synthetic observations from the model with our actual observation, and thus to estimate the *posterior* law of the model parameters around our target.

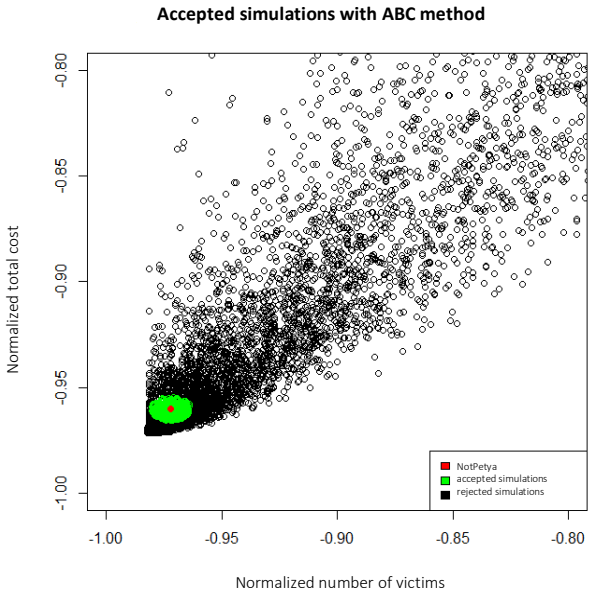


Figure 3 – Acceptance zone with ABC method (1st model)

We have set up three sets of *prior* laws from which we have derived three different statistical models. The behavior of the estimated models are studied. We chose the third model, which not only allowed us to reproduce NotPetya but also all events linking NotPetya to WannaCry (figure 4). Our model is therefore able to generate three types of events: high individual severity and low-range events (NotPetya), low individual severity and high-range events (WannaCry), or new central events that we consider to be probable since they are located between NotPetya and WannaCry.

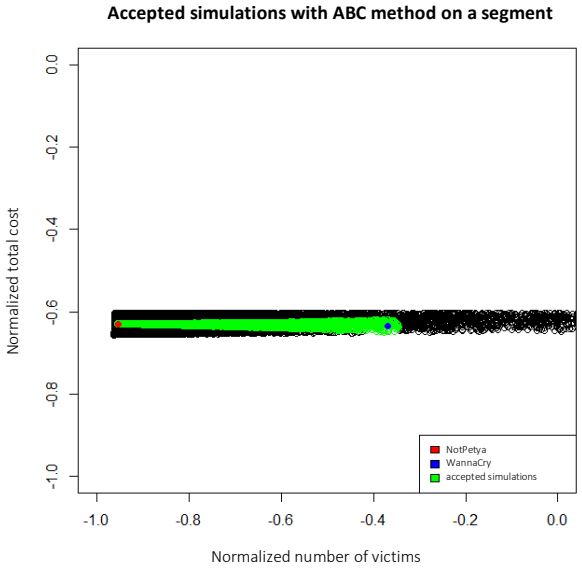


Figure 4 - Acceptance zone with ABC method on a segment (3rd model)

We proceed using bootstrap on parameters accepted by ABC algorithm to simulate the model according to the *posterior* law. To carry out the simulations, we randomize hyperparameters fixed for the

estimation and analyze the impact of each of these hyperparameters on our simulations. The simulations thus carried out enable us to answer the following question: "What would have happened if NotPetya or WannaCry ransomwares or a hybrid ransomware between these two had targeted another operating system, if the cost of the ransom had been higher and if the attack had not been contained as fast? ».
This model does not allow us to replicate or predict the behavior of any type of ransomware on our portfolio. Nevertheless, it allows to simulate variants close to NotPetya or WannaCry under more adverse conditions, which can be qualified as disaster scenarios.
We study these generated events and calculate the 99.5% quantile of the insured loss at AXA Group level and derive results at entity level. We also explain how this scenario could be integrated into the AXA Group's cyber internal model.

Advantages, limitations and future work

Finally, we have identified the advantages and disadvantages of the model and suggested ways to improve it. The model presented meets our initial objective since it complements the AXA portfolio's vision of the risk carried by the AXA portfolio on cyber affirmative First Party insurance policies. It requires different variables from the cloud scenario to assign a notion of risk to insured companies, which helps diversify the vision of risk held by policyholders.
The construction of the model and the estimation method leverage of the small amount of data available while maintaining a consistent approach. The estimation method may be repeated if new events occur or if a fictitious event representing future fears is to be taken into account.
However, it should be kept in mind that the present model does not have a high accuracy since we have used many proxies to approximate some variables not present in our databases but used by the model. In addition, we do not recommend following our estimation method on smaller portfolios. Indeed, the estimation method is applied conditionally to the companies in the AXA portfolio. The latter being sufficiently large and diversified, it represents the global economy relatively well. For smaller or non-diversified portfolios, the method would not allow events such as NotPetya or WannaCry to be replicated. Since cyber-attacks are often happen very quickly, the classic use of an epidemiological model to anticipate the progression of a virus in order to better stop it, is difficult here, but can still be implemented by insurers to try to evaluate an upper bound of their loss in the event of a new ransomware.
We studied the impacts of the model parameters and variables through correlation matrices and graphs. Further sensitivity testing would be interesting to conduct. Given the structure of the economic cost function, we expect a high positive sensitivity of the model to policyholders' revenues, a variable to which the cloud model was quite insensitive. The model could be enriched with more precise information on policyholders to avoid the use of proxies. It will then be interesting to study the evolution of results. Thanks to the model's structure it will be possible to incorporate risk scores on policyholders when they become available.

Table des matières

Introduction

Les premiers contrats d'assurance cyber ont été vendus dans les années 1990 aux États-Unis. Depuis, le marché de l'assurance cyber ne cesse de progresser. Cette croissance de la demande en couvertures cyber résulte autant de la réglementation accrue en termes de protection des données que du rôle central que tiennent aujourd'hui les systèmes informatiques dans notre société. Ces deux facteurs poussent les agents à transférer leur risque vers l'assureur. Bien que le marché de l'assurance cyber soit aujourd'hui très profitable, les (ré)assureurs placent le risque cyber au premier rang des risques émergents. Les (ré)assureurs redoutent principalement une accumulation de sinistres provoqués par un même évènement ou attaque cyber. Ces craintes sont parfaitement illustrées par les deux attaques ransomware, WannaCry et NotPetya, ayant eu lieu respectivement en mai et juin 2017. En l'espace de quelques heures, des milliers d'entreprises et institutions du monde entier ont été contaminées par un virus informatique paralysant leur activité. Les pertes mondiales causées par ces deux évènements sont estimées respectivement à 8 et 10 milliards de dollars.

L'objectif principal de ce mémoire est la construction d'un nouveau scénario d'accumulation à intégrer au modèle interne cyber. Nous parlerons d'évènement d'accumulation lorsqu'un même évènement ou attaque cyber touche au moins deux polices d'assurance distinctes.

Le caractère évolutif du risque cyber pousse les assureurs à adapter les contrats qu'ils proposent. Ainsi, chaque assureur doit construire et suivre l'évolution de sa propre nomenclature pour gérer ses contrats et appréhender au mieux son risque. La qualité des données récoltées lors de la souscription influe sur la modélisation et la gestion des risques. En effet, la bonne gestion des données relatives aux polices d'assurance favorise une modélisation précise du risque réellement porté par l'assureur.
Le risque cyber étant un risque nouveau, les bases de sinistres des assureurs disposent d'un faible historique. Par conséquent, l'assureur n'est pas en mesure de construire ses modèles à partir de sa propre expérience acquise à travers les sinistres survenus sur son portefeuille. Les sinistres d'un portefeuille sont en effet peu représentatifs du risque cyber. Pour compléter ses bases et renforcer ses connaissances, l'assureur peut recourir à des bases de données externes recensant des évènements cyber. L'utilisation de ces bases de données externes soulève des questions de fiabilité et d'absence d'exposition au risque. Ces bases sont difficilement utilisables telles quelles pour construire tout un modèle avec une approche fréquence/sévérité. Elles peuvent néanmoins servir à vérifier certaines hypothèses ou conjectures utilisées dans les modèles de l'assureur.
Les phénomènes d'accumulation vont à l'encontre de la mutualisation des risques, qui est un principe primordial de l'assurance. Une modélisation classique supposant l'indépendance entre la fréquence et la sévérité est donc à proscrire pour modéliser des évènements d'accumulation. Pour évaluer l'impact qu'aurait une catastrophe cyber sur son portefeuille, il est préférable pour l'assureur de procéder à une approche par scénario.

Ce rapport est organisé en trois parties. Dans une première partie nous présenterons le contexte de l'étude. Nous proposerons une définition du risque cyber avant de déduire les spécificités de ce risque. Nous dresserons le cadre réglementaire et expliquerons son influence sur le marché de l'assurance cyber. Ce marché sera présenté avec ses principales garanties et perspectives de croissance. Le cadre spécifique de l'étude et les données à disposition seront présentés.
Dans une seconde partie, nous présenterons la structure du modèle cyber actuel et le scénario dont il est muni : une attaque de serveur cloud. Nous montrerons ensuite notre approche pour intégrer au

modèle interne un portefeuille de coassurance obtenu auprès d'une entité AXA. A travers ces travaux, nous montrerons l'importance de la qualité des données. Nous comparerons aussi la perte produite par notre modèle interne à la perte engendrée par un scénario externe que nous avons implémenté.
La troisième et dernière partie sera consacrée à la modélisation d'un nouveau scénario pouvant être incorporé au modèle cyber. Nous proposerons une analogie entre cyber et pandémie pour modéliser la propagation d'un malware (programme informatique malveillant). Nous prendrons soin de justifier ce choix avant de présenter quelques modèles épidémiologiques compartimentaux puis de construire notre modèle. Nous construirons le scénario ransomware à l'aide de données que nous avons recensées sur l'attaque la plus dévastatrice jusqu'à présent : NotPetya. Le cadre bayésien sera ensuite utilisé pour mettre nos connaissances à profit lors de l'estimation des paramètres du modèle. Plusieurs jeux de lois *a priori* induisant différents modèles statistiques seront proposés. Nous choisirons ensuite un modèle que nous utiliserons pour simuler la perte assurée. Enfin, les avantages et limites de notre modèle seront établies avant de proposer des pistes de travaux complémentaires.

Chapitre 1
Contexte de l'étude

1.1 L'origine du risque cyber

1.1.1 Définition

Le progrès informatique et technologique amène avec lui de nouveaux risques regroupés sous le nom de « *cyber risk* » que nous allons définir plus précisément. Une étude de l'APREF (Association des Professionnels de la Réassurance en France) [1] qualifie le cyber risque comme étant « pour toute personne morale ou physique, ci-après désignée comme « l'entité » 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 chaines logistiques / sous-traitants)
- une atteinte à la marque et/ou à la réputation de l'entité »
Le risque cyber regroupe des atteintes faites tant aux données qu'aux systèmes électroniques résultant d'un acte volontaire ou involontaire ayant pour conséquence tout type de dégâts.

1.1.2 Importance du risque cyber et bref historique d'attaques

La définition proposée recouvre un large panel d'évènements. Il nous semble donc intéressant de montrer le rang que tient le risque cyber parmi d'autres menaces et de fournir au lecteur quelques exemples d'évènements cyber.

La FFA (Fédération française de l'assurance) a publié en 2019 la deuxième édition du baromètre des risques émergents pour le secteur de l'assurance et de la réassurance en France. Le cyber risque figure en première position pour la deuxième année consécutive [2], devant les tensions sociales et la crise du système financier (figure 1). A horizon 5 ans le risque cyber reste aussi premier, cette fois ci devant le réchauffement climatique et la crise du système financier (figure 2).

Figure 1 - Classement des risques en 2019

Figure 2- Classement des risques à horizon 5 ans

Le risque cyber apparait donc aux yeux des assureurs et des réassureurs comme étant le risque principal susceptible d'impacter considérablement leur activité. L'ampleur de ses conséquences économiques et géopolitiques inquiète fortement les divers acteurs.

L'intensification du risque cyber résulte de nombreux facteurs tels que la numérisation de l'économie, l'augmentation du nombre de données collectées, la globalisation de l'économie et l'accroissement de l'inter-connectivité des secteurs d'activité. La concurrence accrue dans le secteur de la tech joue aussi un rôle important. Des systèmes voulus toujours plus performants ont peu de temps pour être testés avant d'être commercialisés.

Les systèmes informatiques tiennent une place importante dans notre société. Des secteurs clés comme l'énergie, les transports ou encore la santé sont petit à petit devenus dépendants des systèmes informatiques. L'automatisation de certaines tâches a permis un gain de précision et de rapidité certain, mais a aussi rendu notre société dépendante des systèmes informatiques. Tout dérèglement voire interruption peut causer des dégâts considérables.

Le rôle central des systèmes informatiques dans la gestion des entreprises est aussi à souligner, puisqu'ils stockent et véhiculent des informations stratégiques et confidentielles et sont un outil de travail majeur de notre époque. Leur utilisation est devenue quasi indispensable dans la plupart des secteurs d'activité, si bien que leur indisponibilité ou leur dégradation entrainent des pertes considérables.

Afin de mieux comprendre les craintes liées à ce risque, nous proposons maintenant au lecteur un bref historique d'évènements cyber. Ci-dessous en Figure 3 une frise chronologique établie par SCOR P&C relatant divers évènements cyber entre 2016 et 2018 [3]:

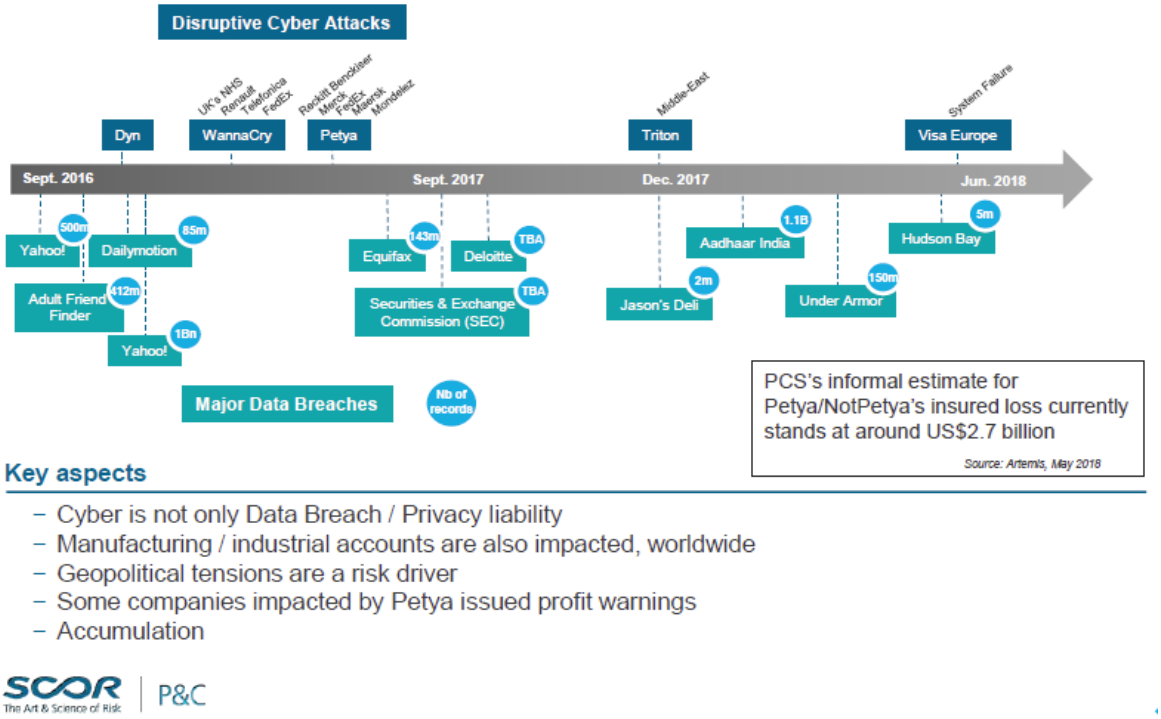


Figure 3-Chronologie des évènements cyber

Décrivons plus en détail quelques évènements de la frise :
Attaques malveillantes

-**Dyn** (octobre 2016) est une attaque par déni de service (ou DoS pour 'Denial of Service attack') visant le service Dyn Managed DNS. Ce service gère les adresse IP dynamiques de certains sites comme Twitter, Netflix, Ebay, Github ou Paypal qui ont été rendus inaccessibles durant une dizaine d'heures. Une DoS consiste à empêcher les utilisateurs légitimes d'un service de l'utiliser. Souvent ce type d'attaque est produite à partir de plusieurs sources (on parle alors de DDoS pour 'Distributed Denial of Service attack') qui cherchent à saturer le réseau de la cible pour perturber son fonctionnement.

-**WannaCry** (mai 2017) est un ransomware, c'est-à-dire un virus informatique qui une fois infiltré bloque l'utilisation de l'appareil informatique et chiffre son contenu avant de demander une rançon à l'utilisateur pour procéder à une hypothétique décontamination et récupération des données.
Ce ransomware a infecté environ 300 000 appareils informatiques dans 150 pays et exigeait une rançon comprise entre 300USD$ et 600USD$. Il a exploité une faille de sécurité présente sur des systèmes non mis à jour opérant sur des versions de Windows antérieures à Windows 10. Cette faille aurait dans un premier temps été utilisée par la NSA avant de tomber aux mains de hackers. Il semblerait que les premières infections aient eu lieu en Espagne ou au Royaume-Uni avant de se répandre au reste du monde en quelques heures. A ce jour, deux hypothèses subsistent quant au mode de transmission : la première suppose que des pièces jointes contaminées auraient été envoyées dans un grand nombre d'e-mails tandis que la seconde mise sur le caractère auto répliquant du virus qui se serait propagé via des honeypots (un honeypot est un leurre servant à attirer des potentiels hackers sur un serveur ou programme afin de mieux étudier leurs ressources et les neutraliser).
Au Royaume-Uni, le système de santé a été impacté : des rendez-vous annulés, des ambulances déviées, et quelques opérations annulées. Des grandes entreprises et organisations comme Vodafone, FedEx, Renault, Telefonica ou encore Deutsche Bahn ont été touchées. La perte totale est estimée à 8 milliards de dollars. Le gain pour les auteurs de WannaCry est inférieur à 150 000USD$, ce qui semble peu comparé au trouble provoqué dans l'économie.

-**NotPetya** (juin 2017) est un *wiper (effaceur en anglais)*, c'est-à-dire un logiciel malveillant détruisant les données, qui apparait sous la forme d'un ransomware. Tout comme WannaCry, NotPetya exploite une faille informatique, mais cette fois-ci pour toute version de Windows non mise à jour. Au sein des entreprises, il s'active à partir d'un fichier .exe, puis une fois un ordinateur infecté, il se développe via le réseau interne. Si ce réseau interne est connecté à des partenaires, le virus les infecte aussi.
Des grandes entreprises comme Saint-Gobain, Merck et Maersk ont été touchées et comptabilisent chacune des pertes entre 250 et 300 millions d'euros. L'armateur danois Maersk a notamment dû réinstaller 4 000 serveurs, 45 000 ordinateurs, 2 500 applications en l'espace de 10 jours. Le géant pétrolier russe Rosneft a dû passer sur des serveurs de secours. La centrale nucléaire de Tchernobyl a elle aussi été impactée par le virus, et les mesures de radioactivité ont dû être suivies manuellement. La perte totale est estimée à 10 milliards de dollars.

Intrusion et vol de données confidentielles

-En 2014, **Sony Pictures Entertainment** a été victime d'une attaque visant à dérober des données confidentielles ; des données portant principalement sur les salariés et les scripts de film ont été volées, puis diffusée publiquement sur Internet. Cette même année, **Orange** a vu les données personnelles de 1.3 million de clients être volées.

-En 2016 **Yahoo!** a reporté un vol de données d'environ 1 milliard de comptes. Ce piratage aurait eu lieu entre 2013 et 2014. Verizon qui était sur le point d'acquérir Yahoo! a négocié un rabais de 350 millions de dollars sur le prix d'origine.

-En 2017 **Equifax**, une agence de notation de crédit, a été victime d'un piratage durant 2 mois et demi [4]. Au cours de cette période, 145.5 millions d'individus ont été concernés par un vol de données confidentielles comme le nom, le numéro de sécurité sociale, la date de naissance, le numéro de permis de conduire. En une attaque, c'est un peu moins de la moitié de la population américaine qui a potentiellement vu ses données personnelles dérobées.

Bugs et erreurs de système

-En juin 2018 **Visa Europe** a vu ses systèmes de paiement tomber en panne pendant environ une heure. Ceci a causé le refus d'environ 5.2 millions de transactions [5]. Visa a affirmé que cette panne n'était en aucun cas due à une intrusion ou une quelconque attaque externe mais simplement à un centre de données dont l'interrupteur ne fonctionnait pas correctement.
Afin de comprendre plus en détail le fonctionnement des attaques cyber, nous recommandons au lecteur les parties dédiées à cet effet des mémoires d'Actuariat de Madame Laura SYED [6] et Monsieur Florian PONS [7].

1.2 Les spécificités du risque cyber

À travers les exemples présentés, nous retenons certaines caractéristiques du risque cyber.

1.2.1 Un risque « man made »

Les évènements cyber sont de nature très variée. Les attaques peuvent émaner d'acteurs très différents allant du simple employé à une institution étatique.
Du point de vue de l'attaqué, le risque est aléatoire lorsqu'il s'agit d'un incident non intentionnel ou encore d'une attaque volontaire mais non liée à la nature de la victime.
Quand il s'agit d'attaques volontaires sur des entreprises emblématiques ou des Etats, le risque cyber perd son aspect aléatoire et peut être assimilé au risque politique ou au risque de guerre. En effet, l'attaquant ne choisit pas uniquement sa cible en fonction des chances de succès de son attaque mais est motivé par des raisons pécuniaires ou politiques.

1.2.2 Un risque évolutif

Les hackers utilisent des moyens différents à chaque attaque. Ils adaptent leurs virus pour exploiter les failles présentes dans les systèmes d'information. Aucun programme ou système ne peut garantir le risque zéro car les types d'attaque et les moyens d'infiltration des systèmes informatiques sont en constante évolution. La cybersécurité et la détection d'attaque est rendue difficile par le caractère nouveau de chaque attaque. Pour détecter une attaque, l'informaticien doit repérer des signaux ou des traces laissées par le hacker. Des systèmes automatisés peuvent détecter des signaux basiques (lien de phishing, lien non sécurisé, faux nom de domaine, etc.) et éviter les attaques dont le mode opératoire est déjà connu. Pour le reste, la vérification de l'absence de faille de sécurité via le 'ethical hacking'

(pratique qui consiste à tenter d'hacker des systèmes pour évaluer les potentielles brèches et failles) est primordial.

1.2.3 Un risque systémique et contagieux

La portée maximale d'une attaque est difficilement délimitable. WannaCry et NotPetya illustrent que le risque cyber est sans frontière et doté d'une grande vitesse de propagation. Même les acteurs les mieux protégés peuvent être des victimes collatérales d'une contamination extérieure. Les attaques peuvent par exemple exploiter une vulnérabilité d'un logiciel très répandu ou encore dégrader les structures d'un opérateur dominant sur le marché, ce qui in fine aura un impact à l'échelle planétaire. Une attaque cyber peut toucher un à plusieurs milliers d'ordinateurs dans le monde entier et donc causer des petits dégâts isolés comme des dégâts simultanés très importants. Denis KESSLER, PDG du groupe SCOR, a présenté le risque cyber comme étant aussi important que le risque de catastrophe naturelle [8].
Nous parlerons de phénomène d'accumulation lorsqu'une attaque (ou un accident) est à l'origine de dégâts pour au moins deux assurés.

1.2.4 Un risque imprévisible, invisible et latent

Divers acteurs, avec des pratiques et des motivations variées, sont susceptibles d'attaquer des systèmes informatiques. Contrairement à d'autres risques où l'assureur peut faire de la veille sur des indicateurs, le manque de données et le caractère évolutif du risque rend difficilement possible une telle pratique pour le risque cyber.
La prévention semble pouvoir éviter les attaques de faible portée, visant une entreprise en particulier. Cependant, dès lors que l'attaque vise un système très répandu, il est difficile de prévoir l'ampleur de la contamination et la manière dont le virus va se propager avant d'être endigué. Comme en témoigne Visa, les entreprises peuvent aussi être sujettes à des pannes totalement imprévues de leurs systèmes informatiques.
Contrairement à d'autres sinistres comme le vol, les conséquences directes d'une attaque cyber ne sont pas toujours évidentes. Il existe en effet un certain temps de latence ou d'incubation entre le début de l'attaque et sa détection. Une fois détectée, il est parfois difficile d'estimer les dégâts précis. La victime peut s'apercevoir plus tard que des données cruciales ont été altérées lors de l'attaque. Cet aspect du risque cyber doit être pris en compte pour le calcul des réserves.

1.3 Le cadre réglementaire

Le caractère systémique et global du risque cyber encourage les pays du monde entier à se munir de réglementations. Face aux menaces cyber, les Etats mettent en place des lois visant à protéger leurs citoyens et leurs entreprises. On distingue l'obligation de notifier des obligations de renforcement de la sécurité informatique. Nous allons rappeler par zone géographique les différentes lois en vigueur.
Avant cela, donnons la définition d'un *data breach* qui est une brèche de sécurité des données, c'est-à-dire un vol, une destruction, une utilisation ou un accès non autorisé à des données conservées par une entreprise ou une institution.

1.3.1 Les Etats Unis

Concernant la protection des systèmes et des données, les Etats Unis ont été les premiers à légiférer. Le « Health Insurance Portability and Accountability Act » (HIPAA) de 1996, le « Gramm-Leach-Billey Act » de 1999 et le « Homeland Security Act » 2002 obligent respectivement les institutions de santé, bancaires, et les diverses entités de l'Etat à protéger leurs systèmes d'information.
Les Américains sont aussi les pionniers en matière de législation sur la notification. En 2003, le « Notice of Security Breach Act » adopté en Californie, oblige les entreprises à informer leurs clients en cas de fuite de données personnelles les concernant. La Californie sera suivie par de nombreux Etats dans les années suivantes.

1.3.2 L'Europe

La Politique de l'Union Européenne tend à renforcer les capacités nationales de sécurité et à augmenter la collaboration entre les pays membre en matière de lutte et de collecte d'information concernant le risque cyber. Pour ce faire, l'UE a intensifié son action avec la fondation de la ENISA (European Union Agency for Network and Information Security) en 2004 [9]. Cette organisation d'aide européenne a pour mission d'assurer un niveau élevé de sécurité et de protection des réseaux et de l'information en intervenant en collaboration avec les instances nationales et les institutions de l'Union Européenne.
La directive NIS (Network and Information System Security) a pour objectif d'assurer un niveau de sécurité élevé et commun à tous les pays de l'Union Européenne. Cette directive entrée en vigueur depuis aout 2016 a accordé un délai de 21 mois aux pays membres de l'UE pour transposer les éléments de la directive dans leur législation nationale. En France, c'est l'ANSII (l'agence nationale de la sécurité des systèmes d'information) qui veille à établir un cadre réglementaire conforme à l'esprit de la directive NIS [10].
Le RGPD (Règlement Général sur la Protection des Données, ou GDPR en anglais) mis en application depuis mai 2018 renforce la protection des données pour les individus au sein de l'UE. Ce règlement impose notamment aux entreprises et divers organismes de notifier l'autorité nationale de protection en cas de violation graves, afin que les utilisateurs puissent prendre des mesures appropriées. Il garantit aussi aux particuliers la protection, l'effacement ou encore de portabilité de leurs données personnelles. En France, c'est la CNIL (Commission Nationale de l'Informatique et des Libertés) qui veille au respect de la RGPD.

1.3.3 L'Asie

La volonté de mettre en place une régulation pour la protection des données semble assez récente en Asie. Certains pays comme la Chine (« The Personal Information Security Specification », mai 2018), l'Inde (Right to Privacy Law, 2014), l'Indonésie (« The Operation of Electronic Systems and Transactions », 2012) et la Thaïlande (« Personal Data Protection Bill », mai 2018) disposent de textes visant à la protection des données, mais il n'existe pas de régulateur à l'échelle nationale pour veiller à l'application des lois et sanctionner le cas échéant.
Hong Kong, les Philippines, l'Australie, et la Nouvelle-Zélande disposent de régulateurs et sanctionnent financièrement en cas de non-respect des règles, notamment celle de notifier (jusqu'à 1.8 million USD$ en Australie). En Corée du Sud, les entreprises de télécommunication doivent avoir une assurance ou des réserves suffisantes en cas de vol de données. Des amendes peuvent aller jusqu'à 20 000 USD$, et l'entreprise victime d'un *data breach* doit prouver sa non négligence [11].

1.3.4 Impacts de la réglementation sur l'assurance cyber

Bien qu'il soit difficile de quantifier l'impact direct de ces législations sur l'assurance cyber, nous pouvons tout de même établir deux conséquences majeures de la rigidification des lois.

La première conséquence est la prise de conscience de l'existence d'un tel risque. Les différents acteurs économiques mesurent le poids du risque cyber et prennent peu à peu des précautions pour s'en protéger. L'assurance cyber fait partie des solutions pour réduire ce risque et pourrait donc voir son marché croitre.

La seconde répercussion est l'intensification du nombre de données liées à des évènements cyber. En effet, les nombreuses obligations de notifier permettent peu à peu d'obtenir des bases de données conséquentes. Les assureurs doivent tout de même prendre en compte certains biais dans les données. D'une part, l'augmentation du nombre de données récoltées n'est pas suffisante pour établir l'intensification du risque cyber. Ce phénomène de troncature doit être pris en compte pour l'éventuel calcul d'une loi de fréquence. D'autre part, les entreprises souhaitent souvent minimiser l'impact d'un évènement cyber afin d'éviter une perte de réputation. Pour le calcul d'une loi de coût, l'assureur doit garder à l'esprit que certaines pertes peuvent être divulguées à la baisse. Les données doivent être traitées avec précaution, en prenant en compte la manière dont elles sont récoltées. Un biais, certes difficilement quantifiable, peut être incorporé aux données.

1.4 Le marché de l'assurance cyber

Après avoir listé les principales caractéristiques du risque cyber et rappelé la réglementation en vigueur, nous allons maintenant introduire le marché de l'assurance cyber. L'assurabilité sera d'abord vérifiée, puis les différents types de garanties seront expliquées. Les perspectives de croissance du marché seront énoncées avant d'expliquer comment les assureurs appréhendent ce risque nouveau.

1.4.1 Assurabilité

Avant même d'étudier le marché de l'assurance cyber, nous pouvons nous interroger sur la légitimité de l'existence d'un tel marché. Pour qu'un risque soit assurable, rappelons qu'il doit :

-être mutualisable
Le caractère systémique du risque et la corrélation des risques lors d'attaques majeures pausent question sur le caractère mutualisable d'un tel risque. En effet, la plupart des agents utilisent des outils informatiques similaires et sont donc vulnérables simultanément en cas d'attaque sur l'un de ces systèmes. L'assureur doit tenter de diversifier au maximum son portefeuille selon des critères que nous développerons en 1.4.4.

-être aléatoire
Pour qu'un risque soit assurable, il doit être aléatoire et indépendant de la volonté de l'assuré.
La majorité des attaques sont volontairement causées par un agent extérieur. Le succès d'une attaque dépend considérablement du profil de l'assuré, et des moyens du ou des attaquants. Dans certains cas,

les assurés peuvent constituer des cibles emblématiques et donc être en permanence sujettes à des attaques. Le caractère aléatoire est alors questionnable.
Les incidents causés involontairement par une négligence humaine vérifient le critère aléatoire mais ne représentent pas la majorité des cas (27% dans l'étude « 2018 Cost of Data Breach Study : Global Overview [12]).

-être quantifiable
Le manque de données constitue un obstacle pour quantifier le risque. La profondeur des bases de données des assureurs est plutôt limitée, et souvent avec peu de sinistres. Ceci est dû à la volonté des entreprises de protéger leur réputation. Ces dernières pouvaient avoir tendance à taire ou bien minimiser l'impact d'un évènement cyber, avant que l'obligation de notifier n'entre en vigueur.

-présenter un aléa moral limité
Les assureurs veillent à ce que les agents, une fois assurés maintiennent un niveau d'effort suffisant en termes de cyber sécurité. Ceci se fait souvent via des partenariats avec des acteurs de la cyber sécurité, au moyen d'une notation annuelle du profil de risque permettant d'ajuster le tarif (on pense par exemple au partenariat entre Allianz et Thalès ou encore AXA avec SecurityScorecard et Airbus). La crainte générale concernant le risque cyber pousse aussi les agents à éviter toute négligence en matière de cyber sécurité. Ainsi, on assiste rarement à des négligences volontaires mais plutôt à un manque de connaissances des assurés face aux menaces cyber. Les franchises présentes sur la plupart des contrats incitent aussi l'assuré à une plus grande vigilance.

-présenter une anti sélection limitée
Il est difficile pour l'assureur d'effectuer un audit complet des pratiques et des systèmes informatiques de l'assuré, et in fine de distinguer efficacement les bons risques des mauvais risques. Même les partenariats avec des experts en cybersécurité ne permettent pas (pour un coût raisonnable), de connaître en détails toutes les pratiques d'un assuré. Rappelons que la négligence humaine (exploitée via le « social engineering » qui consiste à tirer parti d'une une faille comportementale humaine) est un facteur important dans l'apparition d'une faille de sécurité d'un système informatique. Cet article « 3 attaques de social engineering auxquelles vous n'auriez jamais pensé » [13] donne 3 exemples de piratage basés sur du social engineering. Sa lecture pourrait donner au lecteur une bonne illustration du *social engineering.*

1.4.2 Les différents types de contrats d'assurance cyber

Plusieurs facteurs poussent les agents à recourir à un contrat d'assurance cyber. Le caractère évolutif du risque cyber incite les agents à se prémunir contre des types d'attaque encore inconnus et par conséquent non traités par leurs systèmes de sécurité. Le caractère systémique et contagieux du risque ne laisse à aucun agent le sentiment d'être invulnérable à une attaque cyber. Pour répondre aux besoins spécifiques de leurs clients, les assureurs proposent plusieurs types de garanties.

Du point de vue de l'assureur, une bonne classification des garanties constitue une première étape importante dans la gestion des risques. L'assureur doit en effet être en mesure de recenser efficacement les garanties vendues afin de savoir quelle police est susceptible d'être impactée selon les types d'évènements.

On distingue tout d'abord les garanties affirmatives des garanties silencieuses:

-les couvertures affirmatives
Comme leur nom l'indique, ces contrats couvrent explicitement le risque cyber résultant par exemple d'accidents informatiques de nature accidentelle ou malveillante et entrainant des dommages matériels ou autres pertes.
-les couvertures silencieuses
Certaines branches d'assurance proposent des garanties tous risques sans exclure explicitement des pertes pouvant résulter d'un évènement cyber. Par exemple, un incendie ou une explosion peuvent être causés par une attaque cyber et sont couverts par une police dommages tous risques. Ce type de garantie dite silencieuse a pour le moment peu été exercée mais pose tout de même question quant à l'exposition totale des assureurs au risque cyber.

Au sein des contrats cyber affirmatifs ou silencieux, il faut aussi différencier les couvertures dites « First Party » des couvertures « Third party » :
-les couvertures *First Party*
Cette catégorie de contrats couvre les dommages matériels et immatériels subis par l'assuré, par exemple le vol ou la destruction de données, l'extorsion de fonds ou encore l'interruption d'activité.
-les couvertures *Third Party*
Cette catégorie de contrats indemnise les pertes subies par un tiers au titre de la responsabilité civile de l'assuré engagée à la suite d'un évènement cyber comme par exemple une erreur dans un programme informatique causant des pertes à des tiers.

Voici une liste de couvertures cyber dont nous allons détailler quelques garanties :

-Business Interruption
-Contingent Business Interruption
-Cyber Ransom and Extortion
-Data Software and Loss
-Financial Theft and Or Fraud
-Incident Response Cost
-Physical Asset Damage
-Regulatory and Legal Defense Costs
-Reputational Damage
-Bodily Injury and Death
-Breach of Privacy, Compensation Costs
-Communication and Media
-Directors and Officers Liability
-Environmental Damage
-Intellectual Property and Theft
-Network Security, Security Failure
-Product and Operations
-Professional Services Error and Omissions
-Tech Errors and Omissions

-Business Interruption ou perte d'exploitation :
Cette garantie indemnise l'assuré pour une perte de revenu liée à l'interruption d'activité résultant d'un évènement cyber.

-Contingent Business Interruption ou perte d'exploitation contingente :
Cette garantie rembourse l'assuré pour des pertes dues à l'interruption d'activité d'un tiers lors d'un évènement cyber.

-Data Software and Loss ou reconstitution de données :
Remboursement des frais de restauration et/ou remplacement de données et/ou de logiciels volés, endommagés, cryptés ou encore supprimés.

-Cyber Ransom and Extortion ou rançon et extorsion de fonds :
Remboursement des rançons payées (pour décrypter des données par exemple) et des extorsions de fonds résultant d'un évènement cyber (hacking de comptes bancaires par exemple).

Dans le cas d'un ransomware, l'assureur déconseille fortement de payer les rançons demandées. En effet, il n'y a aucune certitude que les données soient décryptées après le paiement de la rançon.

-Regulatory and Legal Defense Costs ou frais de défense réglementaire et juridique :
Il s'agit ici d'indemniser l'assuré pour des coûts supportés afin de répondre à des demandes de renseignements réglementaires concernant un évènement cyber. Ceci inclut par exemple les services légaux, informatiques ou techniques.
Rappelons que seule les activités licites sont assurables. Un assureur ne peut donc en aucun cas rembourser les amendes et pénalités dues par exemple au non-respect de la divulgation d'un *data breach* dans les délais fixés par la loi. Il peut en revanche contribuer à indemniser les victimes faisant des réclamations en justice.

-Tech errors and omissions ou erreur technologique et omission :
Lorsque les services fournis par l'assuré sont erronés ou omis, ceci peut entrainer des pertes considérables à des tiers dont l'activité est liée à l'assuré. Si cette garantie est souscrite, l'assureur rembourse donc ces pertes générées.

-Incident Response Cost ou coût de réponse à l'incident :
Remboursement des coûts directement liées à un incident cyber. On pense par exemple aux frais d'investigation puis de nettoyage des systèmes informatiques ou encore de réinstallation de programmes endommagés. Souvent, le coût des mises à jour payantes supprimant la vulnérabilité présente sur les anciens systèmes n'est pas pris en compte.

1.4.3 Perspectives de croissance

Les premiers produits d'assurance couvrant le risque cyber sont apparus aux Etats Unis dans les années 1980-1990. Ils concernaient principalement la responsabilité liée à la diffusion de contenu en ligne erroné à la suite de la compromission d'un logiciel. Ces garanties intervenaient à partir des contrats de responsabilité civile et séduisaient principalement les entreprises du secteur des nouvelles technologies (et les entreprises dites *« point com »* (ou *dot com* en anglais)).
Les premiers contrats d'assurance couvrant la responsabilité envers des tiers à la suite d'une atteinte aux données (*data breach* en anglais) ont été créés dans les années 2000. A l'origine, ces contrats ne prenaient pas en compte les pertes *First Party*. C'est au milieu des années 2000 que la couverture « First Party » a été ajoutée pour assurer les pertes dues à l'extorsion, la perte d'exploitation ou encore les systèmes endommagés.
Rappelons que l'évolution du cadre réglementaire est corrélée à la naissance et la prolifération des contrats d'assurance cyber. En effet, un cadre réglementaire strict sanctionnant financièrement les entreprises en cas de fuite de données client ou autre pousse ces dernières à souscrire une assurance cyber pour transférer une part du risque vers l'assureur. De nouveaux produits d'assurance voient donc le jour, comme par exemple des couvertures de frais d'investigation, de notification ou encore d'assistance aux victimes.
Le marché de l'assurance cyber était estimé à 4 milliards de USD$ de primes brutes émises au niveau mondial en 2018, d'après Munich Ré [14]. La totalité du marché Property and Casualty (P&C) est estimée à 2 trillions de USD$. [15]. Le cyber représente donc une niche de seulement 0.2% de la totalité du marché P&C.
Aux Etats Unis, une soixantaine de compagnies proposent des produits cyber. Ce marché est fortement concentré dans les mains de trois acteurs principaux : AIG, Chubb et XL Group. Ces trois assureurs

américains collectaient à eux seuls 45% des primes américaines en 2015. Le marché américain pesait 3 milliards de USD$ en 2016. En France, le volume total de primes représente environ 80 millions de USD$ au sein d'un marché européen d'environ 300 millions de USD$. En Asie, on estime le total des primes collectées à 50 millions de USD$.
Entre 2013 et 2018, le Loss Ratio des couvertures cyber affirmatives était estimé à 50% [11]. La majorité des sinistres déclarés étaient des attritionnels, ce qui fait pour l'instant du cyber affirmatif un marché parmi les plus profitables.

Dans les prochaines années, le marché de l'assurance cyber devrait poursuivre sa croissance. Selon les projections de Munich Ré, le marché pourrait représenter 8 milliards de dollars de primes brutes en 2020 et 20 milliards en 2025 [14]. L'Europe et l'Asie devraient peu à peu combler leur retard sur les Etats Unis. En Asie, seules 8% des entreprises sont actuellement couvertes contre des attaques malveillantes.
La taille de l'entreprise semble être un facteur déterminant dans la répartition des entreprises couvertes. En France par exemple, 75% des entreprises du CAC 40 ont souscrit à un contrat cyber, contre 40% des sociétés du SBF120 et 5% des PME [16]. La croissance du marché de l'assurance cyber passera donc aussi par la capacité à intéresser un plus large panel de clients. La médiatisation des évènements cyber fait prendre conscience aux agents de l'existence d'un tel risque, ce qui augmente par conséquent la demande en assurance. D'un côté les assurés exigent des tarifs bas avec des limites les plus élevées possible. De l'autre les souscripteurs doivent réussir à gagner des parts de marché tout en maîtrisant l'exposition au risque. La crainte d'un évènement mondial incite les assureurs à imposer des limites relativement basses comparées à la demande en assurance. Si les limites restent trop faibles, les entreprises préfèreront opter pour d'autres stratégies internes de réduction du risque. Pour que les limites augmentent, les assureurs doivent être en mesure de se réassurer. A l'heure actuelle, les réassureurs proposent principalement des traités proportionnels avec des limites annuelles ou par évènement. Une meilleure connaissance du risque pourrait encourager les réassureurs à proposer une offre de traités plus large, ce qui permettra aux assureurs de développer leur activité cyber.
L'assurance cyber pour les particuliers séduit aujourd'hui principalement les clients fortunés. Elle sera sans doute amenée à évoluer et intéresser une plus grande partie de la population avec l'apparition des maisons connectées ou encore des véhicules autonomes.

Nous retenons donc que le marché de l'assurance cyber est en pleine croissance. Son expansion est tant géographique que structurelle avec l'apparition de nouvelles garanties et types de clients. Pour favoriser davantage sa croissance, il serait intéressant de faire migrer l'assurance cyber d'un marché spécialisé vers un marché standardisé. On peut imaginer que les biens digitaux et informatiques pourraient être assurés au même titre que les biens physiques. Il est possible d'estimer le prix d'une usine assurée, pourquoi ne pas faire pareil avec des données ?

1.4.4 Gestion du risque cyber par les assureurs

1.4.4.1 Souscription et diversification du risque

Pour l'assureur, une méthode alternative de diversification s'impose. Contrairement aux risques Catastrophes Naturelles où le principal facteur de diversification est le plus souvent le lieu, le caractère systémique du risque cyber impose la prise en compte d'autres critères de diversification. L'assureur doit tant bien que mal essayer de diversifier le « profil informatique » de ses clients afin de diminuer ses chances de voir la totalité de son portefeuille touché en cas d'évènement d'accumulation.

Lors de la souscription, il peut par exemple demander à ses clients de renseigner :
- le type de serveur
- le fournisseur de serveur, et les entreprises reliées à ce réseau
- le type de système d'exploitation
- le nombre de systèmes informatiques
- la dépendance de leurs activités aux systèmes informatiques
- l'existence de méthodes alternatives de travail en cas d'indisponibilité des systèmes informatiques

Certains assureurs misent sur des partenariats avec des acteurs de la cyber sécurité (comme Allianz/Thalès, AXA/SecurityScorecard [17]) afin d'évaluer le profil de risque de leurs clients plus en détail. Des audits permettent de vérifier si des mesures de sécurité suffisantes sont prises par les clients. Ils pourraient permettre de recenser par la même occasion les systèmes utilisés au sein du portefeuille d'assurés. Ainsi, l'assureur pourrait avoir une connaissance approfondie de son portefeuille et veiller à sa bonne diversification. Cette diversification peut déjà sembler complexe à mettre en œuvre au niveau d'une entité, et l'est encore d'avantage au niveau d'un groupe international.

1.4.4.2 Modélisation du risque

Pour construire une distribution de la perte, le procédé le plus classique est une approche fréquence/sévérité. Pour la mettre en œuvre, l'assureur P&C fait le plus souvent appel à des données collectées sur son portefeuille. Cependant, les données cyber ayant une faible profondeur d'historique, il est intéressant pour l'assureur d'utiliser des données externes. Ces données comportent des biais et leur structure est parfois difficilement exploitable telle quelle. L'exposition relative à chacune de ces bases n'est pas non plus explicite. En effet, les sinistres y sont renseignés sans mentionner avec précision l'univers des agents exposés au risque et susceptibles d'être recensés par la base.
L'assureur doit effectuer un travail conséquent pour utiliser correctement les bases de données externes en corrigeant les biais éventuels liés à la récolte des données ou encore pallier l'absence d'exposition.

Une seconde approche consiste à appliquer des chocs déterministes sur le portefeuille d'assurés. Ces chocs sont souvent des scénarios catastrophes jugés homogènes à une perte bicentenaire. Des chocs moins sévères peuvent aussi aider l'assureur à comprendre comment son portefeuille réagit selon les scénarios possibles. Un choc déterministe jugé homogène à la perte bicentenaire permet à l'assureur de vérifier qu'il respecte son « risk appetite ». Le « risk appetite » peut être définit comme la somme maximale que l'assureur est prêt à perdre pour un niveau de probabilité donné.

Les phénomènes d'accumulation des sinistres vont à l'encontre du principe de mutualisation des risques. En cas de catastrophe, de nombreuses polices risquent d'être impactées au même moment. Un évènement cyber mondial est susceptible de causer des pertes plus importantes par assuré qu'un évènement ciblé sur l'assuré, cela étant en partie lié à une paralysie de l'économie lors d'un évènement majeur. L'hypothèse d'indépendance entre la fréquence et la sévérité est ainsi mise en question. Un évènement d'accumulation aura tendance, selon sa nature, à imputer des pertes de même sévérité aux différentes victimes.

Il va de soi que la gestion des risques est fortement dépendante des informations récoltées lors de la souscription. Plus les informations récoltées sont pertinentes et meilleure est la qualité de recensement de ces données, plus la modélisation du risque sera en mesure de se rapprocher du risque réellement porté par l'assureur.

1.5 Spécificités de notre étude

1.5.1 Contexte Solvabilité II

Dans le cadre de la formule standard de Solvabilité II, il n'existe pas encore de sous module de risque catastrophe spécialement dédié au risque cyber. En effet l'article 119 du « Delegated Act » de 2015 décompose le sous module « risque de catastrophe en non-vie » de la manière suivante :

Article 119

Sous-module «risque de catastrophe en non-vie»

1. Le sous-module «risque de catastrophe en non-vie» est constitué de l'ensemble des sous-modules suivants:

(a) le sous-module «risque de catastrophe naturelle»;

(b) le sous-module «risque de catastrophe en réassurance dommages non proportionnelle»;

(c) le sous-module «risque de catastrophe d'origine humaine»;

(d) Le sous-module «autres risques de catastrophe en non-vie».

2. L'exigence de capital pour le risque de souscription catastrophe en non-vie se calcule comme suit:

$$SCR_{nlCAT} = \sqrt{(SCR_{natCAT} + SCR_{npproperty})^2 + SCR_{mmCAT}^2 + SCR_{CATother}^2}$$

où:

(a) SCR_{natCAT} représente l'exigence de capital pour le risque de catastrophe naturelle;

(b) $SCR_{npproperty}$ représente l'exigence de capital pour le risque de catastrophe en réassurance dommages non proportionnelle;

(c) SCR_{mmCAT} représente l'exigence de capital pour le risque de catastrophe d'origine humaine;

(d) $SCR_{CATother}$ représente l'exigence de capital pour les autres risques de catastrophe en non-vie.

Figure 4 - Article 119 du Delegated Act

Comme nous l'avons évoqué précédemment, le risque cyber est un risque man-made. Afin de vérifier s'il figure dans un sous module, nous devons consulter en détails la composition du sous module « risque de catastrophe d'origine humaine ». Cette information figure dans l'article 128 :

Article 128

Sous-module «risque de catastrophe d'origine humaine»

1. Le sous-module «risque de catastrophe d'origine humaine» est constitué de l'ensemble des sous-modules suivants:

(a) Le sous-module «risque de responsabilité civile automobile»;

(b) le sous-module «risque marin»;

(c) le sous-module «risque aérien»;

(d) le sous-module «risque d'incendie»;

(e) le sous-module «risque de responsabilité civile»;

(f) Le sous-module «risque de crédit et caution».

2. L'exigence de capital pour le risque de catastrophe d'origine humaine se calcule comme suit:

$$SCR_{mmCAT} = \sqrt{\sum_i SCR_i^2}$$

où:

(a) la somme couvre tous les sous-modules visés au paragraphe 1;

(b) SCR_i représente l'exigence de capital pour le sous-module *i*.

Figure 5 - Article 128 du delegated Act

Comme nous pouvons le constater, le risque cyber ne fait pas l'objet d'un sous module à part entière. Le risque provenant des contrats *affirmative Third Party* peut être pris en compte dans le sous module « risque de responsabilité civile ». Le risque cyber induit par des garanties *silent* n'excluant pas explicitement le risque cyber est à prendre en compte directement dans les autres sous modules. Le risque catastrophe cyber lié aux contrats *affirmative First party* ne correspond à aucun module.

Le risque cyber propre à l'assureur, c'est-à-dire lié directement aux systèmes informatiques de l'assureur et non aux contrats vendus, est pris en compte dans le module de risque opérationnel.

1.5.2 Contexte AXA

Chez AXA, des garanties 'affirmative First party' sont vendues et doivent donc faire l'objet d'une modélisation séparée. L'ACPR autorise AXA à s'affranchir de la formule standard et évaluer son risque via son propre modèle interne. AXA doit donc évaluer correctement tous ses risques, y compris ceux ne faisant pas l'objet d'un sous module explicite dans la formule standard.
AXA développe des modèles cyber *First* Party, *Third Party* et Retail. Notre étude est centrée sur les garanties *First Party.*

La principale mission liée à ce stage et à ce mémoire est le passage d'un modèle d'accumulation stochastique basé sur un unique scénario vers un modèle d'accumulation stochastique doté d'un catalogue de scénarios.
Il est en effet plus intéressant pour l'assureur de disposer d'un catalogue de scénarios afin de savoir comment se comporte son portefeuille selon les types d'évènement catastrophe. La distribution obtenue via ce catalogue d'évènements lui permet de mieux appréhender le risque et comprendre comment son portefeuille réagit en cas de scénario catastrophe. Grâce à cette distribution, l'assureur peut étudier tant la perte moyenne générée par un évènement d'ampleur mondiale, que le quantile à 99.5% de cette perte.

Une approche par scénario nous permet d'utiliser une hypothèse de dépendance entre fréquence et sévérité des pertes. En effet, les pertes induites par un même événement d'accumulation sont supposées avoir la même sévérité sur les différents assurés, proportionnellement à leur taille.

Nos travaux ont été effectués au sein de l'équipe Group Risk Management (GRM) Property and Casualty d'AXA, dans un contexte de post-acquisition du groupe XL Catlin. Cette fusion a notamment augmenté considérablement l'exposition du groupe AXA aux risques man-made, dont le risque cyber. Pour mieux connaître son risque et maîtriser son exposition à l'échelle groupe, AXA développe en interne des modèles d'évaluation des risques man-made.

1.5.3 Données à disposition

Présentons les données à disposition pour la rédaction de ce mémoire. Nous explicitons les variables présentes dans chaque base de données et expliquons la présence éventuelle de biais.
Lorsque nous présenterons ces bases, nous garderons à l'esprit les critères d'exhaustivité et d'exactitude des données.

1.5.3.1 Données internes à AXA

Nous avons accès aux données des portefeuilles d'assurance-cyber des entités AXA. Par souci de confidentialité, ces données sont anonymisées et les valeurs numériques sont chiffrées mais les effets observés sont conservés.
Expliquons la nomenclature propre à AXA et qui sera utilisée pour la suite du mémoire. Une police d'assurance cyber est potentiellement composée de deux garanties (ou couvertures) :
- une garantie *First Party*
- une garantie *Third Party*

Les garanties *First* et *Third Party* sont elles même composées de sous-garanties que nous avons présentées en 1.4.2.

Au sein des différents portefeuilles, chaque police est renseignée avec les informations suivantes :
- Identifiant de la police
- Chiffre d'affaires annuel du client
- Secteur d'activité
- Limite de police
- Couvertures souscrites
- Limites de couverture
- Sous-couvertures souscrites
- Limites de sous-couverture
- Priorité
- Déductibles des sous-couvertures
- Primes
- Pays

Les données de sinistre disponibles sont parcellaires et ne concernent pas d'évènements d'accumulation. Nous décidons donc de ne pas les utiliser dans notre étude.
L'enrichissement des bases de données client, permettant notamment d'avoir des informations quant au profil informatique de l'assuré est en cours. Nous n'avons pour le moment pas accès à ces bases enrichies. Le pays, le chiffre d'affaires et le secteur d'activité sont les seules variables que nous pourrons utiliser pour différencier les assurés.
Les primes ne sont pas remplies pour toutes les entités et ne seront donc pas utilisées.

1.5.3.2 Données Open Source

Nous rappelons la définition d'un *data breach* qui est une brèche de sécurité des données, c'est-à-dire un vol, une destruction, une utilisation ou un accès non autorisé à des données conservées par une entreprise ou une institution. On parlera de *mega breach* lorsque plus de 500 000 données seront compromises.
On appellera perte économique ou perte brute d'assurance la perte que subit directement l'assuré. On appellera perte assurée ou perte assurantielle la part de la perte économique sujette à une indemnité.

Veris Community
La base Veris est mise à jour par Verizon depuis 2012.
Cette base utilise l'encodage *one-hot* . L'encodage *one-hot* consiste à représenter une variable qualitative par un nombre de colonnes binaires correspondant aux modalités prises par cette variable. La base non retraitée dispose d'environ 2 400 variables. Les travaux du GRM AXA ont permis de mettre en forme cette base afin de la rendre plus facilement exploitable. Les variables conservées sont notamment :

- le jour de survenance
- le jour de déclaration
- le type d'attaquant (externe, interne)
- le nom du malware
- le type d'attaque
- le type d'équipement touché
- la taille de l'entreprise victime
- le secteur d'activité de la victime
- le nombre de records perdus
- la perte en dollars

Sur son site internet, il est mentionné que la base comporte un biais sectoriel important, puisque presque la moitié des évènements proviennent du secteur de la santé, en particulier du Department of Health and Human Services (HHS). Le biais géographique est lui aussi présent puisque le HHS est une administration américaine.

Institut Ponemon,
Fondé en 2002 par Dr Larry PONEMON et Susan JAYSON, l'Institut Ponemon conduit des recherches indépendantes sur la protection des données et l'émergence des technologies de l'information.
Il publie chaque année une étude intitulée « Cost of Data Breach ». Ces études traitent de pertes économiques dues à des évènements cyber. Dans l'étude 2018, 477 entreprises ont été sondées.
Nous énonçons succinctement quelques faits marquants. Le coût moyen d'un *data breach* est de 3.86 millions de dollars. Ce chiffre est en augmentation par rapport à 2017 (3.62 millions de dollars). Un *mega breach* d'un million de fichiers perdus coûte en moyenne 40 millions de dollars tandis que pour 50 millions de dossiers perdus le coût s'élève à 350 millions de dollars. L'étude suggère qu'il y a une corrélation positive entre le nombre de fichiers perdus et la perte économique. Le temps nécessaire pour identifier la faille et la contenir est lui aussi corrélé positivement avec le coût économique. Ces deux relations nous semblent logiques : une attaque d'une plus grande portée coute plus cher et le temps nécessaire pour réparer les dégâts provoque une interruption d'activité ou une activité partielle. Les actes malveillants causent 48% des *data breaches*, contre 27% pour les erreurs humaines et 25% pour les problèmes de systèmes (du type panne par exemple).
L'étude fournit la répartition par secteurs d'activité des entreprises sondées. La répartition des pays est aussi renseignée et le coût moyen par secteur et par pays est fourni. Ces informations peuvent permettre d'établir un score de sévérité par secteur et pays. Il faut cependant garder à l'esprit que les informations fournies sont sensibles à l'échantillon observé. Par exemple, une première lecture rapide suggère au lecteur que le secteur médical essuie des pertes significativement plus lourdes que les autres secteurs. Cependant, on constate que le secteur médical représente seulement 7 des 477 entreprises sondées. On peut donc s'interroger sur la robustesse des informations qui ressortent de l'étude.

2018 cyber claims study, Net Diligence
Net Diligence fournit annuellement une étude du coût des sinistres cyber, sans pour autant mettre à disposition sa base de données. Cette étude couvre la perte assurantielle et non la perte économique. Les chiffres sont donc difficilement exploitables en l'état car nous ne disposons pas des conditions contractuelles ayant amené à calculer les pertes assurantielles. En gardant bien à l'esprit cet élément, il est tout de même possible de déduire une tendance quant aux évènements cyber qui coûtent le plus cher aux assureurs, et la répartition de leur coût par garantie. Les sinistres étudiés ont eu lieu entre 2013 et 2018.

Breach Level Index (BLI)
Cette base de données est mise à jour par Gemalto, entreprise du groupe Thalès, qui est spécialisée dans le secteur de la sécurité numérique. Les informations contenues dans la base sont collectées depuis des sources publiques, toutes zones géographiques confondues. La période de recensement s'étend de 2013 à aujourd'hui. Pour chaque *breach* recensé, les variables disponibles aujourd'hui sont :
- le secteur d'activité
- la date de l'évènement
- le type d'attaque (vol d'identité, accès aux comptes, accès aux comptes financiers…)
- l'origine de l'attaque (un acteur malveillant, une erreur humaine, une perte physique d'un objet clé…)
- le nombre de fichiers concernés
- la zone géographique touchée
- un score de 1 à 10 pour décrire la gravité de l'attaque (10 étant le plus sévère)

Privacy Right Clearinghouse (PRC)
Privacy Right Clearinghouse est une organisation américaine à but non lucratif dont la mission principale est la protection de la vie privée. Elle produit une base de données recensant les *data breaches* depuis 2005, principalement aux Etats Unis. Elle contient environ 8000 observations et les variables suivantes :
- date de déclaration
- entreprise
- ville
- Etat
- origine de l'attaque/évènement
- type d'entreprise
- nombre de fichiers concernés
- description de l'évènement
- source de l'information avec l'URL
- année de l'évènement
- latitude
- longitude

1.5.3.3 Bases construites et complétées au cours du mémoire

A partir de la base Breach Level Index

Nous partons de la base de données Breach Level Index obtenue par AXA GRM en 2018 via une méthode de *webscraping*. A cette époque, la base fournissait encore comme variable le nom de chaque victime d'un *data breach*. Cette information est précieuse pour trouver d'autres renseignements sur les attaques.

Au cours de ce stage, nous avons en premier lieu voulu compléter cette base internationale riche en informations avec les données financières disponibles sur une base de données externe. Nous avons cherché le chiffre d'affaires et le nombre d'employés de chaque entreprise ou institution ayant subi une perte supérieure à 1000 fichiers perdus.

Il faut noter que les données complétées sont soumises à certains biais :
1) un biais dû aux informations disponibles sur la base de données externe :
- le chiffre d'affaires et le nombre d'employés n'ont pas toujours pu être trouvés, certains types d'institutions publiques (comme par exemple les écoles) ont très rarement ces informations renseignées. Les données de la base externe utilisée sont destinées aux investisseurs, ce qui implique donc une meilleure qualité d'information pour les moyennes et grandes entreprises que pour les petites.
- le chiffre d'affaires renseigné est le plus récent. Cependant lorsque nous renseignons une information nous veillons à ce que le chiffre d'affaire et le nombre d'employés soit assez stable pour l'entreprise étudiée. La base ne permet pas toujours de remonter assez loin dans l'historique des chiffres d'affaires, et certains évènements datent de 2013. Si la taille de l'entreprise est utilisée comme variable catégorielle, ce biais aura peu d'importance.
2) Un biais dû à une troncature volontaire : nous étudions les *data breaches* supérieurs à 1000 fichiers car en dessous de ce seuil, le coût associé ne nous servira pas à modéliser des évènements d'accumulation.

Au cours de cet exercice fastidieux (le webscraping n'étant pas posible sur la base externe utilisée), nous avons pu constater la difficulté de mettre en place une base de données voulue plus complète, en essayant d'y incorporer le moins de biais possible.

Grâce à cette base, il nous est possible d'étudier le nombre de fichiers perdus en fonction du secteur d'activité, du type de compromission, de l'origine de l'attaque, et maintenant de la taille de l'entreprise. Cette démarche est déjà possible dans la base Veris, mais il est intéressant de confronter les sources de données.
Nous appelons cette base complétée BLI_complétée.
Avec plus de temps, nous aurions souhaité compléter de la même manière la base PRC.

Dans un second temps, nous avons essayé d'avoir une meilleure connaissance du coût des *mega breach*. Nous avons donc filtré la base breach level index 2018 en ne gardant que les *data breach* supérieurs à 1 million de fichiers. Nous avons ensuite effectué une recherche internet pour trouver le coût associé à ces *mega breach* et ainsi compléter les informations fournies par l'institut Ponemon. Les entreprises divulguent rarement ces coûts. Le nombre de lignes complétées a donc été faible. Cet apport, certes restreint par notre capacité à trouver l'information, sera tout de même utile pour tester nos fonctions de coût associant le nombre de fichiers compromis à un coût en dollars. Nous appelons cette base BLI *mega breach*.

Les bases Veris, PRC et BLI sont riches en informations mais sont difficilement exploitables pour la construction d'un scénario d'accumulation. Il est en effet difficile de relier des évènements individuels entre eux au sein de ces bases. Ces bases peuvent néanmoins être utilisées pour vérifier certaines hypothèses, ce qui a été fait pour le modèle cloud mais n'est pas présenté dans ce mémoire.

Accumulation
Nous avons créé une base recensant les évènements d'accumulation depuis 2000.
Cette base est évidemment incomplète puisqu'elle est restreinte aux évènements d'accumulation rendus publics et que nous avons pu trouver au cours de nos recherches et lectures. Lorsqu'un évènement est renseigné dans la base, nous essayons de remplir les champs suivants :
- l'année de déclaration
- l'année de commencement

- le type d'attaque
- si une vulnérabilité massive (i.e. une faille de sécurité sur un logiciel où un système d'exploitation très répandu) a été utilisée, si oui laquelle
- la zone géographique touchée
- le coût total en dollars imputé à l'économie
- le coût maximum pour une victime
- le nombre total de victimes impactées
- le type de cible (entreprises, Etats...)
- l'auteur de l'attaque
- si l'évènement apparait dans l'une de nos trois bases principales (PRC, Veris, Breach Level index)
- source : documents et sites internet grâce auxquels les informations sont trouvées

Cette base est utile pour étudier les caractéristiques des évènements d'accumulation et construire des scénarios catastrophe réalistes, en gardant évidemment à l'esprit que les évènements passés ne présagent pas du futur. Elle servira aussi à calibrer une fréquence d'évènements d'accumulation.

Base détaillée d'évènements d'accumulation

Afin d'estimer les paramètres de notre modèle (chapitre 3), nous avons besoin de données précises concernant les attaques cyber. Pour NotPetya, nous avons donc créé une base qui vise à recenser les informations suivantes :
- nombre total de victimes
- coût total pour l'économie
- faille exploitée
- durée de l'attaque
- entreprises touchées (avec chiffre d'affaires, nombre d'employés, secteur d'activité)
- durée de réparation des dégâts
- répartition du coût par postes de dépenses

Les informations trouvées ne sont pas toujours précises mais l'ordre de grandeur sera tout de même une information importante quand il s'agira d'estimer les paramètres de notre modèle dans un cadre bayésien. Par exemple, la durée exacte d'une attaque est difficilement trouvable, mais on parvient à se donner une borne supérieure de cette durée qui se compte en heures, jours ou mois. Une liste exhaustive des entreprises touchées est elle aussi difficilement constituable : on a tendance à trouver plus facilement les pertes les plus élevées touchant de grandes entreprises puisqu'elles sont mieux diffusées par les médias. Lorsqu'il est trouvé pour quelques entreprises, un détail de la répartition du coût résultant d'un évènement cyber permet d'évaluer quelles garanties sont susceptibles d'être touchées et dans quelles proportions selon le type d'attaque.

Conclusion

Dans ce premier chapitre nous avons dressé le contexte de l'étude. Nous avons défini le risque cyber et déduit ses principales caractéristiques à travers des évènements historiques. Nous avons ensuite introduit les différentes réglementations en vigueur et établi leur potentiel impact sur les données open source de sinistres cyber, à savoir l'intensification du recensement d'évènements. Nous avons présenté des éléments de réponse à la question de l'assurabilité et décrit un marché dont la croissance pourrait s'intensifier grâce à une bonne appréhension du risque. Même si le risque cyber ne figure pas

explicitement dans Solvabilité II, nous avons vu qu'il était primordial pour AXA d'évaluer un tel risque. Ce mémoire vise à contribuer à l'évaluation du risque cyber porté par le groupe AXA en enrichissant le modèle interne d'un scénario supplémentaire : le scénario ransomware. Le troisième chapitre utilisera les caractéristiques du risque cyber présentées ici pour construire le modèle de notre scénario ransomware et justifier l'analogie entre cyber et pandémie.
Nous allons maintenant nous familiariser avec le modèle existant en y intégrant un portefeuille de coassurance obtenu auprès d'une entité AXA.

Chapitre 2
Modèle actuel

Nous appelons perte par évènement une perte conditionnée au fait qu'un évènement ait lieu, à ne pas confondre avec la perte annuelle qui correspond à la perte totale sur une année et peut donc prendre en compte la perte relative à plusieurs évènements ou aucun.
Pour chacun des modèles développés dans ce chapitre, on s'intéressera uniquement à la distribution des pertes par évènement.
Dans l'intégralité de ce chapitre, les données utilisées pour appliquer les scénarios sont fondées sur des portefeuilles existants mais ont été significativement altérées. Cela concerne notamment les montant des limites de police, de couverture et la répartition des sous-garanties dans les contrats.

2.1 Le modèle actuel

2.1.1 Structure du modèle

Nous présentons ici brièvement la structure du modèle interne pour le risque cyber *affirmative First Party.*

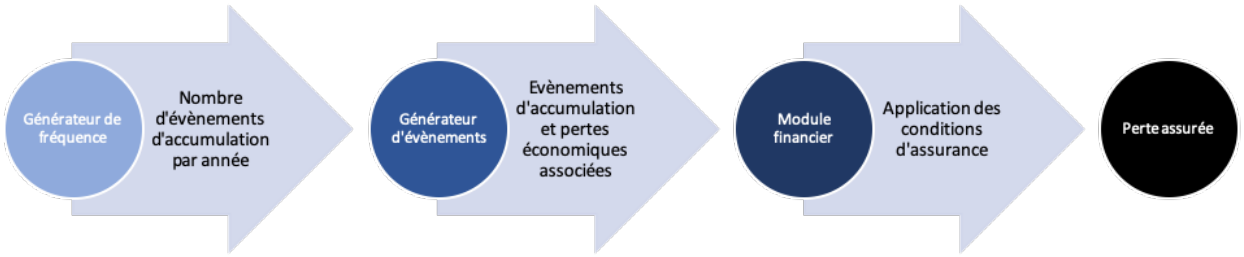


Figure 6 - Structure du modèle interne cyber affirmative First Party

Un premier générateur de fréquence simule le nombre d'évènements d'accumulation N_k ayant eu lieu pendant une année k.
Un second générateur simule des évènements d'accumulation et leurs impacts sur les polices d'assurance. Notons X_j le coût associé à ces évènements.
Pour chaque année k, on tire d'abord une réalisation n de N_k, puis n pertes X_j afin de les sommer et obtenir la perte annuelle.
En notant S_k la charge de l'année k on a donc :

$$S_k = \sum_{j=0}^{N_k} X_j$$

Le modèle suppose l'indépendance entre le nombre d'évènements et leurs coûts.

En revanche, le modèle ne suppose pas l'indépendance entre les coûts d'un même évènement. Si on regarde X_j de plus près on a :

$$X_j = \sum_{i=0}^{M_j} C_i$$

Avec : M_j la variable aléatoire donnant le nombre de polices touchées pour l'évènement j et C_i le coût associé à la $i^{\text{ième}}$ police touchée lors de l'évènement j.
Dans les scénarios établis, les C_i ne sont pas indépendants puisqu'ils dépendent d'une sévérité commune provenant du scénario simulé.
La distribution de la perte annuelle est obtenue en simulant un grand nombre de charges totales S_k.

2.1.2 Le scénario cloud

Au début de ce stage, le modèle était totalement déterministe et doté d'un scénario. Ma première contribution au cours de ce stage a été d'aider au passage d'un modèle déterministe vers un modèle stochastique. J'ai notamment pris part aux discussions amenant à cette modélisation et ai participé à l'implémentation du modèle.

Le scénario cloud n'étant pas l'objet de ce mémoire, nous ne présentons pas en détails le déroulement du scénario mais expliquons brièvement le principe.
Le scénario vise à reproduire sur notre portefeuille les conséquences d'une attaque ayant lieu contre un serveur cloud. En fonction du continent du serveur cloud attaqué, une proportion d'assurés affectés est tirée et voit ses données compromises. L'indisponibilité des données stockées sur le cloud provoque des pertes sur ces polices. La perte économique associée à chaque assuré est déterminé en fonction de sa taille, de son secteur et de la sévérité de l'attaque. Ce coût économique est ensuite ventilé par sous-garanties avant d'appliquer les conditions financières des contrats pour obtenir la perte assurée.

2.2 Utilisation du modèle : intégration d'un portefeuille de coassurance

2.2.1 Présentation du problème

Présentons ici la démarche qui a été effectuée pour estimer à l'aide du modèle interne la perte bicentenaire relative à un portefeuille de coassurance obtenu auprès d'une entité AXA. Sur ce portefeuille de coassurance, l'entité AXA n'est pas l'apériteur mais prend une quote-part de 20% des risques souscrits. Pour simplifier nos références à ce portefeuille, appelons le portefeuille A.
A travers ces travaux nous nous familiariserons avec le modèle interne qui reposait alors sur le scénario cloud déterministe. Nous montrerons aussi l'importance de la qualité des données et à la nécessité pour l'actuaire de savoir fournir une estimation même en l'absence de variables à priori primordiales pour son calcul. Pour aider leurs prises de décisions, les équipes de direction peuvent en effet avoir besoin d'une estimation de la perte bicentenaire alors que les données à disposition ne permettent pas un calcul précis.
Nous allons ici décrire notre approche pour fournir une estimation de la perte bicentenaire et l'évolution de cette estimation au fur et à mesure que nous avons reçu un complément d'informations sur le

portefeuille de coassurance. Ce portefeuille étant essentiellement européen, nous utiliserons un portefeuille d'assurance européen, appelé portefeuille B, pour calibrer les modèles donnant les variables manquantes, ce qui suppose que les deux portefeuilles A et B soient relativement similaires.

2.2.2 Première base de données et premiers résultats

2.2.2.1 Présentation des données

Dans un premier temps, nous avons eu accès à une base de données du portefeuille A où les variables suivantes étaient disponibles :

- Nom de l'assuré
- Ligne de Business
- Date Début/Fin couverture
- Limite de couverture
- Priorité
- Primes
- Secteur d'activité

Dans notre base de données du portefeuille B que nous allons utiliser comme référence, les variables suivantes sont à disposition :

- Identifiant de la police
- Chiffre d'affaires
- Secteur
- Priorité
- Limite de couverture
- Sous-garantie souscrites
- Limite de sous-garantie
- Déductible de sous-garantie

- Les secteurs d'activité renseignés ne suivent pas la même nomenclature que ceux utilisés par AXA, un travail de correspondance a donc dû être effectué.
- Nous rappelons que le chiffre d'affaires est une variable utilisée dans le scénario cloud et constatons qu'il est totalement absent de la base. Le premier objectif est donc de construire un proxy du chiffre d'affaires en fonction d'autres variables communes aux deux bases afin de pouvoir calibrer un modèle, puis estimer le chiffre d'affaires des assurés du portefeuille.
- Notons aussi que la base de données fournie ne détaille pas du tout les garanties contrats. Nous aurons donc à estimer une distribution des couvertures du portefeuille A.
- Pour simplifier le problème, on va supposer que les déductibles de couverture sont nuls et on s'attend donc à avoir des estimations prudentes.

Rappelons que dans notre portefeuille B, les informations ne remontent pas plus haut que la maille couverture : nous n'avons pas la limite de police mais cette dernière n'est de toute façon pas utilisée car on se restreint à un scénario touchant les garanties *affirmative First Party*. Nous n'avons pas non plus accès aux primes, cette variable présente dans la base du portefeuille A ne pourra donc pas être utilisée pour construire un proxy du chiffre d'affaires. Nous pensons que les primes auraient été une bonne variable explicative du chiffre d'affaires de l'assuré dans la mesure où elles traduisent l'espérance de la perte (en théorie et modulo des chargements complémentaires), et que cette espérance dépend en partie de la taille de l'entreprise.

2.2.2.2 Estimation du chiffre d'affaires

Nous décidons d'estimer le chiffre d'affaires en utilisant la priorité et la limite de couverture comme variables explicatives et distinguons différents modèles par secteur. Nous construisons nos modèles sur le portefeuille B avant de les appliquer au portefeuille A pour obtenir les variables manquantes.

- Modèle Linéaire

Pour construire un premier modèle simple de référence nous choisissons un modèle linéaire. Pour étudier la robustesse de ce modèle nous procédons par validation croisée. Nous utilisons la méthodes k-folders cross-validation avec k=5. Ainsi, à chaque itération le modèle apprend sur 80% des données (train set) et est testé sur les 20% restant (test set). Certains secteurs étant peu représentés et la base présentant un grand nombre de lignes, nous risquons d'avoir des tirages où un secteur est absent de la base d'apprentissage et présent dans la base test (ou en trop faible nombre pour estimer un modèle). Pour éviter ces cas, nous procédons à une stratification sur la variable secteur à chaque tirage. Ainsi, chaque échantillon tiré conserve la même proportion d'entreprises par secteur que la base d'origine. Un modèle linéaire peut alors être estimé pour tout secteur à chaque itération. On a donc pour une entreprise j du secteur i :

$$CA_j = \beta_i^0 + \beta_i^1 \times LC_j + \beta_i^2 \times P_j + \varepsilon_j$$

Avec :
j l'identifiant de l'entreprise j parmi les n_i entreprises du secteur i,
CA_j , LC_j, P_j, respectivement le Chiffre d'Affaires, la Limite de Couverture et la Priorité de l'entreprise j,
$\beta = (\beta_i^0, \beta_i^1, \beta_i^2)$ les paramètres du modèle linéaire pour le secteur i,
ε_j le résidu de l'entreprise j.

Disposant de 24 secteurs d'activité et donc de 24 modèles, nous choisissons de détailler les résultats d'un de ces 24 modèles obtenus. Regardons d'abord un résumé du modèle estimé en Figure 7 avant de s'intéresser à la validation des hypothèses du modèle linéaire grâce à la Figure 8.

```
Call:
lm(formula = TotalInsuredTurnover ~ ., data = data[Sector ==
    20, c("Limit", "Attachment", "TotalInsuredTurnover")])

Residuals:
       Min         1Q     Median         3Q        Max
-1.345e+10 -2.632e+08 -2.632e+08 -2.632e+08  2.578e+10

Coefficients:
             Estimate Std. Error t value Pr(>|t|)
(Intercept) 2.738e+08  4.656e+07    5.88 4.93e-09 ***
Limit       1.759e+02  1.184e+01   14.85  < 2e-16 ***
Attachment  9.144e+01  6.482e+00   14.11  < 2e-16 ***
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1

Residual standard error: 1.88e+09 on 1671 degrees of freedom
Multiple R-squared:  0.2052, Adjusted R-squared:  0.2042
F-statistic: 215.7 on 2 and 1671 DF,  p-value: < 2.2e-16
```

Figure 7 - Résultats de la régression linéaire

On retient les informations suivantes des résultats obtenus avec R :
- Les coefficients testés individuellement sont non nuls. En effet, pour chaque coefficient le test de Student renvoie des p-valeurs très faibles, nous rejetons donc H0 au seuil de confiance 5%. On rappelle que dans le cadre du test de Student pour la significativité des coefficients de régression linéaire,

l'hypothèse nulle H0 « le coefficient testé est nul » est testée contre l'hypothèse alternative H1 « Le coefficient testé est différent de zéro ».

- Le modèle estimé a un R^2 de 0,2052 ce qui est assez faible. Le modèle explique à lui seul uniquement 20% de la variance des observations[1].

- Le modèle estimé est significatif. En effet, le test de Fisher renvoie une p-valeur inférieure à 10^{-15}. La statistique de Fisher permet ici de comparer le modèle réduit à l'intercept au modèle estimé au moyen de la régression linéaire. H0 est « le modèle estimé n'est pas significatif et chacun des coefficients sauf l'intercepte vaut 0 » tandis que H1 est « le modèle estimé est significatif et les coefficients estimés sont non nuls ».

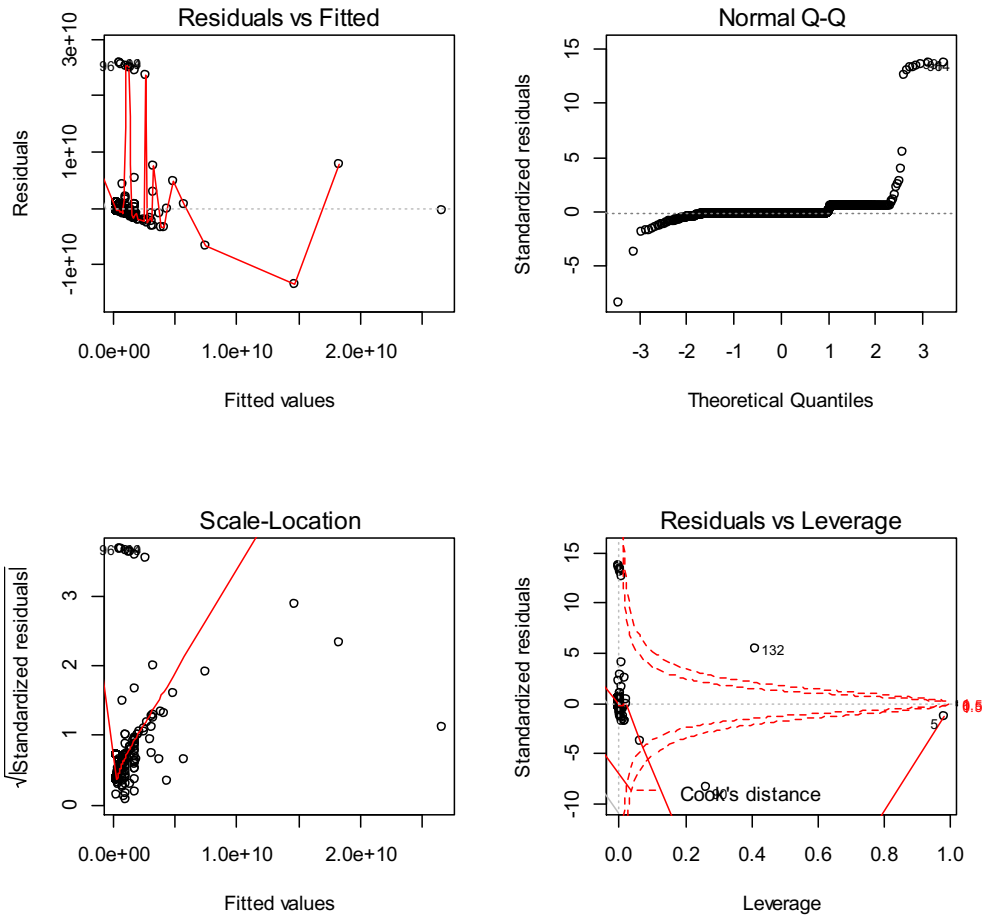


Figure 8 - Graphiques de validation des hypothèses du modèle linéaire gaussien homoscédastique

Les graphiques précédents permettent de tester les hypothèses du modèle linéaire gaussien :

Hypothèse i) les résidus sont centrés.

Le premier graphique « Residuals vs Fitted » en haut à gauche montre des valeurs assez bien réparties par rapport à la droite d'équation $residuals = 0$. On remarque juste que nos données présentent beaucoup de petites valeurs à prédire et quelques grandes valeurs à prédire.

Hypothèses ii) les résidus sont homoscédastiques.

Le graphique « Scale-location » donnant les résidus standardisés suggère une relation de croissance entre les résidus et le chiffre d'affaires. On rejette l'hypothèse d'homoscédasticité.

[1] On rappelle que le coefficient R^2 vaut $\frac{SCM}{SCT}$ ou encore $1 - \frac{SCR}{SCT}$ en présence d'un intercept.
$SCM = \sum_{k=0}^{n}(\widehat{y_k} - \bar{y})^2$; $SCT = \sum_{k=0}^{n}(y_k - \bar{y})^2$; $SCR = \sum_{k=0}^{n}(\widehat{y_k} - y_k)^2$; n le nombre d'observations ; y_k la valeur prise par l'observation k ; $\widehat{y_k}$ la valeur prédite par le modèle pour l'observation k ; $\bar{y}$ la moyenne des n observations.

Hypothèses iii) les résidus sont indépendants.
On ne peut pas vérifier cette hypothèse car elle dépend de la manière dont sont récoltées les données.
Hypothèses iv) : les résidus sont gaussiens.
Le graphique « Normal Q-Q » présentant les quantiles empiriques en fonction des quantiles théoriques de la loi normale ne donne pas une droite. On a par ailleurs un groupe de quantiles théoriques à 15 contre 3 pour la valeur théorique. On rejette donc très clairement l'hypothèse de normalité des résidus.

Les évaluations des modèles linéaires calibrés sur les autres secteurs sont semblables à celle-ci.
Nos modèles ne vérifient pas toutes les hypothèses d'application du modèle linéaire gaussien, il faudrait notamment prendre en compte l'hétéroscédasticité.
Il peut sembler contradictoire d'avoir un modèle significatif (hypothèse de nullité des coefficients systématiquement rejetée) dont le R^2 est faible. Cela signifie en réalité que nos modèles captent peu d'information (sans doute à cause du faible nombre de variables explicatives) mais que cette faible quantité d'information n'est pas négligeable.
Si on utilise l'erreur quadratique moyenne (ou sa racine carrée) pour évaluer nos modèles nous concluons qu'ils sont très mauvais. En effet, voici ci-dessous un tableau donnant la racine carrée de l'erreur quadratique moyenne selon les itérations de validation croisée :

Root MSE[1]	Itération 1	Itération 2	Itération 3	Itération 4	Itération 5
Train	6 429 721 496	6 360 995 060	6 379 684 634	6 516 092 371	6 134 461 606
Test	6 667 743 005	5 073 387 648	5 077 700 932	4 329 440 376	6 191 214 367

Tableau 1- Résultats de la validation croisée

Nous nous trompons donc en moyenne de 5.4 milliards de dollars de chiffre d'affaire annuel sur l'échantillon test, ce qui est très élevé. Nos modèles produisent parfois des chiffres d'affaires négatifs que nous remettons à zéro par soucis de cohérence.
Dans le scénario cloud on utilise le chiffre d'affaires pour affecter une taille catégorielle à l'entreprise assurée : nous n'avons donc pas besoin d'un degré de précision très élevé mais d'un ordre de grandeur pour affecter la bonne taille à l'assuré. Pour obtenir cette taille, une première correspondance est effectuée entre le chiffre d'affaires et le nombre d'employés : on divise le chiffre d'affaires de l'assuré par le chiffre d'affaires moyen produit par employé. Ce chiffre d'affaires moyen varie selon les secteurs. La variable nombre d'employés obtenue est ensuite rendue catégorielle au moyen de la table suivante :

Number of employee	Company size category
0 à 10	1
11 à 100	2
101 à 1 000	3
1 001 à 10 000	4
10 001 à 50 000	5
Supérieur à 50 001	6

Tableau 2- Classification de la taille d'entreprise en fonction du nombre d'employés

[1] *Root Mean Squared Error* $= (\frac{1}{n}\sum_{k=0}^{n} (\widehat{y_k} - y_i)^2)^{1/2}$ avec $\widehat{y_k}$ la prédiction et y_i la vraie valeur à prédire pour chacun des i individus parmi les n étudiés.

Si nous utilisons le chiffre d'affaires prédit pour construire cette variable qualitative de la taille de l'entreprise, notre problème revient à une classification supervisée à 6 modalités. Nous allons donc voir si la faible variance captée par le modèle permet de construire un classifieur satisfaisant.
Pour évaluer la qualité du classifieur, nous calculons l'erreur de classification[1]. Nous regardons aussi si les mauvaises classes prédites ont tendance à être des classes plus ou moins grandes que la classe réelle, afin de savoir si notre modèle est conservateur ou non.
On note P la prédiction et O l'observation réelle de la taille catégorielle de l'entreprise. Le tableau suivant présente les pourcentages de cas pour lesquels la taille prédite est inférieure, égale, ou supérieure à la classe observée.

En %	Itération 1			Itération 2			Itération 3			Itération 4			Itération 5		
	P<0	*P=0*	*P>0*	*P<0*	*P=0*	*P>0*	*P<0*	*P=0*	*P>0*	*P<0*	*P=0*	*P>0*	*P<0*	*P=0*	*P>0*
train	5.9	76.3	17.8	6.0	76.3	17.6	6.9	76.4	17.7	5.1	77.1	17.8	6.8	75.4	17.8
test	6.5	76.1	17.4	5.7	76.3	18.0	6.4	75.9	17.7	5.1	76.7	18.2	6.0	76.2	17.8

Tableau 3- Evaluation de la prudence du classifieur à chaque étape de la validation croisée

Le tableau suivant donne la moyenne des résultats obtenus sur les 5 itérations.

En %	Moyenne des 5 itérations		
	P<0	P=0	P>0
train	6.1	76.3	17.7
test	5.9	76.2	17.8

Tableau 4-Moyenne des résultats de la validation croisée

Sur l'échantillon d'apprentissage et test nous avons respectivement une précision moyenne de 76.3% et 76.24%. Ces deux pourcentages étant proches, nous pensons donc que le modèle est robuste et n'est pas sujet au sur-apprentissage. De plus, le modèle a tendance à être prudent, tant sur la base d'apprentissage que sur la base de test. Nous garderons cet élément à l'esprit quand il s'agira d'analyser nos résultats.

Lorsque nous estimons un seul modèle linéaire tous secteurs confondus, le pourcentage de bonnes classes est en moyenne de 6.2% sur l'échantillon d'apprentissage et de 6% sur l'échantillon test. Ceci confirme l'intérêt de différencier les modèles par secteur.
L'influence du secteur sur le chiffre d'affaires annuel peut aussi être montrée au moyen d'une analyse de la variance. Les résultats de l'Anova sont fournis ci-dessous :

```
> model_anova <-aov(TotalInsuredTurnover~Sector, data)
> summary(model_anova)
              Df    Sum Sq   Mean Sq F value Pr(>F)
Sector         1 6.411e+22 6.411e+22    1398 <2e-16 ***
Residuals  30889 1.416e+24 4.584e+19
---
Signif. codes:  0 '***' 0.001 '**' 0.01 '*' 0.05 '.' 0.1 ' ' 1
```

Figure 9 - Anova avec R

On observe une p-value inférieure à 2^{-16} : l'hypothèse H0 de nullité des coefficients par secteur est rejetée au seuil de confiance 5%. On rappelle que l'Anova permet de tester si une variable qualitative (ici le secteur) a de l'influence sur une variable à prédire (ici le chiffre d'affaires).

[1] On définit ici l'erreur de classification comme étant : $\frac{1}{n}\sum_{i=0}^{n} 1_{\{x_i \neq c_i\}}$ avec x_i le label prédit et c_i la vraie classe à prédire pour chacun des i individus parmi les n étudiés.

Pour obtenir le modèle final, nous calibrons les paramètres des 24 modèles linéaires sur la totalité des données et obtenons donc 24 vecteurs de 3 coefficients. Le chiffre d'affaires des entreprises du portefeuilles A seront estimés à partir de ces coefficients.

Nous avons donc vu que les modèles linéaires n'expliquaient qu'une faible partie de la variance et semblaient mauvais. Mais si on utilise ces modèles dans le cadre de notre classification de taille d'entreprise, le classifieur obtenu est assez performant et prudent. Il semble robuste dans la mesure où les résultats sur les bases de test sont toujours très proches de ceux sur la base d'apprentissage. Avant de valider l'utilisation de ce modèle sur le portefeuille A pour ensuite estimer la perte bicentenaire, nous étudions les performances d'autres modèles.

- K Nearest Neighbors

Nous essayons maintenant d'entrainer un algorithme des K plus proches voisins sur nos données. Comme pour le modèle linéaire, nous procédons au estimation de modèles différents par secteur. On décide d'utiliser l'algorithme de régression des K plus proches voisins pour estimer le chiffre d'affaires et ensuite déduire la taille de l'entreprise via nos deux étapes de correspondance. On aurait aussi pu directement utiliser l'algorithme de classification des K plus proches voisins.

Le calibrage du modèle consiste ici à choisir K tel que l'erreur de prédiction du classifieur sur l'échantillon test soit minimisée.
Comme pour le modèle linaire, nous utilisons une validation croisée couplée à une stratification. Encore une fois, la méthode de validation croisée utilisée est la k-folders cross-validation avec k=5.
Pour chaque K on calcule l'erreur moyenne de classification des 5 itérations sur l'échantillon d'apprentissage et sur l'échantillon test. On note que l'erreur minimale pour l'échantillon test correspond à K=1 (cette erreur vaut évidemment zéro sur l'échantillon d'apprentissage puisqu'une entreprise est associée uniquement à elle-même). L'erreur de prédiction étant minimale pour de très faibles valeurs de K, la stabilité du modèle pose question, on écarte donc assez vite ce modèle et on décide de ne pas explorer d'autres algorithmes d'apprentissage statistique.

Nous choisissons d'utiliser le modèle linéaire obtenu précédemment que nous jugeons plus stable et dont l'erreur de prédiction était assez proche d'une méthode des KNN.

2.2.2.3 Simulation d'une répartition des garanties

Notons N le nombre de sous-garanties par police d'assurance.
Sur notre portefeuille B, on a $E(N)=2.36$ et $Var(N)=0.97$
On veut répliquer cette distribution des sous-garanties sur le portefeuille A, pour ensuite être en mesure d'évaluer une perte bicentenaire via l'application du scénario cloud.

- Tirage individuel des sous-garanties

Le tableau suivant présente le nombre de sous-garanties souscrites dans le portefeuille B :

Sous-garantie[1]	Nombre de polices avec la sous garantie	probabilité	Limite de sous garantie (m USD$)	Limite de couverture (m USD$)	$\frac{\text{Limite de sous garantie}}{\text{Limite de couverture}}$
CYL	5 890	0,96	12 764	10 392	0,81
BI	1 255	0,20	15 869	14 647	0,92
CBI	183	0,03	4 080	1 416	0,35
IRC	516	0,08	6 174	5 353	0,87
RLD	514	0,08	6 162	5 382	0,87
FTT	28	0,00	204	174	0,85
RPD	4 568	0,74	2 664	2 589	0,97
CRE	714	0,12	7 738	7 125	0,92
PAD	812	0,13	4 631	4 510	0,97
Total	14 481	1,00	60 286	51 588	0,86

Tableau 5-Répartition des sous-garanties dans le portefeuille B

Nous avons au total 6 135 polices d'assurance dans le portefeuille B. Donnons quelques explications sur le contenu du tableau. Pour une police donnée, la probabilité d'avoir une sous-garantie souscrite est le nombre de polices avec la sous-garantie divisé par le nombre total de polices. Pour CYL on a par exemple : 5 890/6 135 = 0.96. Ces probabilités sont renseignées dans la colonne probabilité.
La colonne Limite de sous-garantie est la limite moyenne des sous-garanties tandis que Limite de couverture est la moyenne des limites de couverture pour lesquels la sous-garantie est souscrite. La dernière colonne est le quotient de ces deux quantités. Ce tableau va nous permettre de tirer aléatoirement des couvertures pour chacune des polices du portefeuille A, et d'affecter une limite de sous-garantie à ces contrats.

Pour chaque police dans le portefeuille A :
- on réalise 9 tirages indépendants de variables aléatoires de Bernoulli de paramètres respectifs les probabilités d'apparition de chacune des sous-garanties. Pour les tirages réussis, la sous-garantie correspondante est affectée à la police.
- les limites des sous-garanties affectées sont déterminées en multipliant la Limite de Couverture de la police (information connue) par le ratio $\frac{\text{Limite de sous garantie}}{\text{Limite de couverture}}$ de la sous-garantie correspondante.

Sur le portefeuille A ainsi complété, on obtient *E (N) = 2,35* et *Var(N) = 0,78.*
Simuler individuellement les sous-garanties des polices ne prend pas en compte la dépendance des sous-garanties entre elles au moment de la souscription, les variances de N ne coïncident donc pas. Par conséquent on décide de tirer les sous-garanties par groupes et non plus indépendamment les unes des autres.

- Tirages par groupe de sous-garanties
Pour mieux coller aux données du portefeuille d'assurance, on décide de tirer les sous-garanties non plus de manière indépendante mais directement par groupe. On cherche donc dans un premier temps la distribution de chaque groupe possible. Pour 9 sous-garanties, on a 511 groupes possibles. (Somme des combinaisons $\sum_k \binom{9}{k} = 511$) Dans notre portefeuille B, nous avons uniquement 44 groupes dont nous calculons la fréquence d'apparition puis déduisons une probabilité.

[1] CYL correspond ici à Data Software and Loss, BI-Business Interruption, CBI-Contingent Business Interruption, IRC-Incident Response Cost, RLD-Regulatory and Legal Defense Costs, FTT-Financial Theft and or Fraud, RPD-Reputational Damage,CRE-Cyber Ransom Extorsion, PAD-Physical Asset Damage.

Pour chaque police dans le portefeuille A :
- on tire un groupe de sous-garanties avec une loi discrète basée sur les probabilités d'apparition de chaque groupe de sous-garanties.
- on calcule les limites de sous-garanties en multipliant la limite de couverture de la police (information connue) par le ratio $\frac{\text{Limite de Sous-garantie}}{\text{Limite de Couverture}}$de la sous-garantie correspondante évoqué précédemment.
Sur le portefeuille A ainsi complété, on obtient *E(N) = 2.36* et *V(N) =0.98.*

2.2.2.4 Premiers résultats

Nous avons à disposition les variables nécessaires pour calculer la perte associée au scénario cloud. Afin de prendre en compte la quote-part de 20%, la perte totale assurée est calculée avec la limite de couverture multipliée par 5, puis 20% de cette perte est imputée à notre portefeuille A.

Base de données	Expo 1st Part (€)	Perte 1st Part (€)	Destruction Rate
1ère Base: modèles linéaires avec tirages indépendants	1 245 860 697	31 247 104	0.025
1ère Base: modèles linéaire avec tirages par groupes	1 245 860 697	27 745 687	0.022

Tableau 6- Pertes selon la méthode de simulation des sous-garanties

Bien que ces résultats soient proches, ils semblent indiquer une dépendance à la répartition des sous-garanties dans les contrats. La perte assurée fait en effet intervenir une limite de police commune aux sous-garanties d'une même police. La perte assurée dépend donc de l'association des sous-garanties au sein des polices. Prenons un exemple extrême pour illustrer ce phénomène. Pour les contrats où les sous-garanties fortement impactées par le scénario figurent : si les sous-garanties fortement impactées par le scénario sont toujours uniquement associées à des sous-garanties non touchées par le scénario, alors la perte par police sera le montant de la sous-garantie capée par la limite de police. Si au contraire les sous-garanties impactées par le scénario sont toujours regroupées avec au moins une autre fortement impactée au sein d'une même police, alors la perte assurée sera la somme des pertes par sous-garanties captée à la limite de police. Avec notre première méthode de tirage indépendants, on a une perte de 31 millions. Avec la seconde méthode de tirages par groupes, on a une perte de 27 millions. Nous pensons que cette différence est due au fait que les garanties les plus impactées par le scénario sont plus souvent tirées ensemble avec le tirage par groupes qu'avec le tirage indépendant et donne donc une perte inférieure pour le tirage par groupes.
Pour cette première base de données, nous retiendrons les résultats correspondant au tirage par groupe car nous supposons que les stratégies de souscription des deux assureurs sont similaires. Nous analysons la répartition des pertes dans le tableau suivant :

Sous-garantie	Nombre de sous-garantie	Limite moyenne (€)	Perte moyenne (€)	Importance dans scenario cloud	% de la perte totale	Perte par sous-garantie (€)
BI	595	65 843	2 819	46%	30%	8 391 975
RLD	246	76 273	851	17%	4%	1 044 711
CYL	2 798	69 834	1 200	11%	60%	16 790 453
IRC	246	70 707	1 233	26%	6%	1 518 549
Total						27 745 687

Tableau 7- Résultats pour la première base : pertes par garanties

Nous garderons à l'esprit que la garantie la plus présente est CYL et qu'elle représente 60% des pertes alors que seulement 11% de la perte économique lui est affectée dans le scénario cloud.

2.2.3 Seconde base de données et résultats finaux

Peu de temps après nos premières estimations, nous avons reçu des informations complémentaires quant à la structure du portefeuille A.
Une nouvelle base contenant les variables suivantes nous a été transmise :

- identifiant de la police
- limite de couverture
- déductible de couverture
- les sous-garanties souscrites
- les limites des sous-garanties
- le secteur d'activité
- la taille de l'entreprise (Large ou Small)

N'ayant plus accès à la priorité dans cette base et n'étant pas en mesure de faire une correspondance avec l'ancienne base, nous calibrons de nouveaux modèles linéaires par secteur permettant d'estimer le chiffre d'affaires de l'assuré en fonction de la limite de Couverture et du Déductible de Couverture. Les modèles estimés semblent moins bons (environ 60% de bonnes classifications) mais restent prudents. Nous garderons à l'esprit ce changement de modèle au moment d'analyser les résultats. Les sous-garanties et leurs limites ne sont plus à simuler.
Nous obtenons les résultats suivants :

Base de données	Expo 1st Part (€)	Perte 1st Part (€)	Destruction Rate
2ème Base: modèles linéaires avec covariables différentes	1 412 018 518	72 712 227	0.051

Tableau 8-Premiers résultats pour la seconde base de données

Avec cette seconde base de données, on obtient une perte 2.6 fois plus élevée qu'avec la première. Identifions les facteurs qui pourraient expliquer cette différence :
- la mauvaise estimation du chiffre d'affaires (nos deux modèles sont conservateurs lorsqu'ils ne sont pas justes et le second modèle est moins précis que le premier : on surestime donc plus souvent le chiffre d'affaires).
- le nombre moyen de sous-garanties est plus élevé que celui simulé : 4.39 contre 2.35 et les garanties réellement souscrites ont une structure différente de celles simulées.

2.2.3.1 Sensibilité au chiffre d'affaires

Les chiffres d'affaires simulés à partir de la seconde base ont une moyenne de 1 137 636 982€ contre 699 779 628€ pour l'ancienne. On décide de multiplier nos chiffres d'affaires simulés dans la seconde base par $\frac{699\ 779\ 628}{1\ 137\ 636\ 982}$ afin de recentrer le chiffre d'affaire simulé sur l'ancienne moyenne et étudier la sensibilité des résultats au chiffre d'affaires. On obtient les résultats suivants :

Base de données	Expo 1st Part (€)	Perte 1st Part (€)	Destruction Rate
2ème Base: modèles linéaires avec covariables différentes	1 412 018 518	72 712 227	0.051
2ème Base: modèles linéaires avec covariables différentes et re-centrage	1 412 018 518	72 680 884	0.051

Tableau 9-Comparaison des résultats avec et sans re-centrage du chiffre d'affaires

En faisant varier la variable chiffre d'affaire de -38%, on obtient une variation de la perte d'uniquement -0.04%. Le ratio $\frac{\%\ Variation\ Perte}{\%\ Variation\ Chiffre\ d'affaires}$ vaut donc 0.1%. Une variation de 1% du chiffre d'affaire des assurés entraine une variation de 0.1% de la perte simulée par le modèle.
Nos résultats sont donc peu sensibles au chiffre d'affaires de l'assuré.

2.2.3.2 Étude des sous-garanties

Nous cherchons à savoir si la répartition différente des sous-garanties est un facteur expliquant le passage à une perte 2.6 fois plus importante que nos premières estimations.
Une première intuition a été de regarder la sous-garantie la plus impactée par le scénario cloud :CBI
On remarque que cette sous-garantie est 4.6 fois plus répandue dans notre seconde base de données que dans la première et avec une limite moyenne en augmentation de 7%.

Base de données	Nombre total de sous-garanties CBI	Limite de CBI (€)
1ère Base	595	430 453
2ème Base	2 807	462 942

Tableau 10-Répartition du CBI dans les 2 bases de données

Cette garantie étant la plus fortement impactée par le scénario, il semble naturel que la perte soit plus importante lorsque le scénario est appliqué à la seconde base de données. Nous décidons d'étudier plus en détails la répartition de la perte par sous-garantie après application du scénario cloud.

Pour la première base :

Sous-garantie	Nombre de sous-garanties	Limite moyenne (€)	Perte Moyenne (€)	Importance dans scenario cloud	% de la perte totale	Perte par sous-garantie (€)
CBI	595	65 843	2 819	46%	30%	8 391 975
RLD	246	76 273	851	17%	4%	1 044 711
CYL	2 798	69 834	1 200	11%	60%	16 790 453
IRC	246	70 707	1 233	26%	6%	1 518 549
Total						27 745 687

Tableau 11-Pertes par garanties pour la première base de données

Pour la seconde base :

Sous-garantie	Nombre de sous-garanties	Limite moyenne (€)	Perte Moyenne (€)	Importance dans scenario cloud	% de la perte totale	Perte par sous-garantie (€)
CBI	2 807	92 588	2 549	46%	41.8%	30 629 300
RLD	3 391	88 132	994	17%	19.7%	14 438 422
CYL	2 660	91 171	633	11%	9.8%	7 204 451
IRC	3 406	162 317	1 441	26%	28.7%	21 015 260
Total						73 287 432

Tableau 12-Pertes par garanties pour la seconde base de données

On remarque tout d'abord que la répartition des sous-garanties simulées et la répartition réelle sont totalement différentes. D'une part en termes de nombre de garanties souscrites par police : on a une moyenne de 2.35 sous-garanties par police pour nos simulations contre 4.36 en réalité. D'autre part en termes de types de sous-garanties souscrites : le portefeuille A contient majoritairement des sous-garanties IRC et CBI, alors que le portefeuille B était principalement constitué de CYL. Cette disparité va à l'encontre de l'hypothèse faite au début de l'étude, à savoir que les portefeuilles A et B auraient à priori une structure proche puisqu'ils proviennent du même continent. Notons que les limites de garanties sont assez proches pour les deux bases de données sauf pour la garantie IRC ou la limite est 1.78 fois plus élevée pour la seconde base.

Une fois ces différences remarquées, il est naturel que le scénario cloud appliqué à la seconde base génère une perte bien plus importante. En effet, les deux garanties les plus touchées par le scénario cloud CBI (46%) et IRC (26%), sont les plus représentées dans le portefeuille A et avec des limites supérieures. IRC apparait 14 fois plus dans la seconde base et avec une limite 1.78 fois supérieure. CBI apparait 4.6 fois plus dans la seconde base et avec une limite 1.07 fois supérieure. Ainsi, CBI et IRC représentent à elles deux environ 70% de la perte totale dans la seconde base tandis qu'elles représentaient 40% dans la première.

2.2.3.3 Résultats finaux

Nous avons déterminé le facteur principal ayant amené à multiplier le bicentenaire par 2.6 entre le passage d'une base de données à l'autre. Nous avons vu que les chiffres d'affaires simulés n'avaient pas une grande influence sur le bicentenaire et que la structure des sous-garanties du portefeuille était le facteur explicatif principal d'une telle augmentation.

Nos modèles linéaires estimant le chiffre d'affaires se comportaient bien sur le portefeuille B, mais comme nous l'avons vu avec la répartition des garanties, les portefeuilles A et B ne semblent pas comparables. Il se pourrait qu'à l'image des sous-garanties, nous ayons très mal modélisé le chiffre d'affaires. Pour vérifier cela, on utilise la variable taille et on assigne un chiffre d'affaires unique à la catégorie Small et un chiffre d'affaires unique à la catégorie Large (on rappelle que dans le portefeuille A, la variable taille est renseignée. Cette variable contient uniquement 2 modalités : Small et Large, faisant référence à catégorisation du chiffre d'affaire provenant d'une étude connue en interne). Ces deux chiffres d'affaires uniques sont calculés de la manière suivante :

- on calcule la médiane des chiffres d'affaires des entreprises du portefeuille B classifiées comme Small dans notre convention, on fait de même pour les Large
- on affecte le chiffre d'affaires Small à toutes les entreprises Small du portefeuille A et le chiffre d'affaires Large à toutes les entreprises Large du portefeuille A.
Avec cette nouvelle adaptation, on obtient les résultats suivants :

Base de données	Expo 1st Part (€)	Perte 1st Part (€)	DR
2ème Base: Chiffre d'affaires catégoriel	1 412 018 518	68 664 876	0.048

Tableau 13-Pertes sur la seconde base avec le chiffre d'affaires comme variable catégorielle

Ce résultat est proche de celui trouvé précédemment, à savoir une variation de -6%.
On teste la sensibilité à cette variable taille en affectant toutes les entreprises à Small puis toutes les entreprises à Large :

Base de données	Expo 1st Part (€)	Perte 1st Part (€)	DR
2ème Base: tout 'Large'	1 412 018 518	81 125 798	0.057
2ème Base: tout 'Small'	1 412 018 518	58 117 949	0.041

Tableau 14-Résultats de la sensibilité à la catégorie de taille d'entreprises

La variable taille donne à elle seule une amplitude de 23 millions d'euros. Cela peut à première vue sembler entrer en contradiction avec notre première conjecture sur la non-sensibilité du modèle au chiffre d'affaires. Mais il faut savoir qu'une entreprise Large a un chiffre d'affaires 249 fois plus élevé qu'une entreprise Small. Pour une entreprise, un passage de Small à Large représente donc une variation de +248%, bien plus importante que les -38% appliqués précédemment.
Un passage de toutes les entreprises Small à toutes les entreprises Large donne le ratio de sensibilité suivant : $\frac{\%\ Variation\ Perte}{\%\ Variation\ Chiffre\ d'affaires} = \frac{(81\ 125\ 798/58\ 117\ 949)\ -1}{248} = 0{,}0015$
On a donc une sensibilité de 0.15% ce qui est en accord avec nos résultats précédents.

On décide de garder comme résultat 68 millions d'euros, en gardant à l'esprit que cette valeur n'est pas exacte mais représente une estimation de la perte bicentenaire.

2.2.3.4 Anticipation des résultats finaux ?

Une question nous vient naturellement à l'esprit : aurions-nous pu anticiper cette variation entre l'estimation sur la première base et celle sur la seconde base ?
Autrement dit, aurions-nous pu trouver un intervalle de confiance autour de notre première estimation de la perte bicentenaire ? Une fois l'intervalle trouvé, l'estimation effectuée sur la seconde base aurait-elle été dans cet intervalle ?

Pour obtenir cet intervalle, plusieurs approches auraient été possibles :
1) Simuler un grand nombre de fois les tirages par groupes de sous-garanties puis appliquer à chaque structure de portefeuille le scénario cloud. Ainsi on obtiendrait une distribution du coût total assuré. Ces tirages seraient effectués en respectant la loi des groupes de sous-garanties, dont le nombre de sous-garantie par police a pour espérance 2.35 et pour variance 0.97. Nous ne pensons pas que cette approche permette de créer une volatilité suffisante pour que le second résultat soit dans les valeurs prises par le coût total assuré simulé puisque toutes nos simulations auraient en moyenne 2,35 sous-garanties par

contrat contre 4,39 sous-garanties par contrat pour la seconde base. Il y aurait encore une trop grande différence de structure entre les deux bases.

2) Simuler les sous-garanties du portefeuille en faisant varier l'espérance du nombre de sous-garanties par police. On aurait pu par exemple se donner une loi de probabilité sur le nombre de sous-garanties par contrat et ajuster la probabilité d'occurrence des groupes (ou des sous-garanties si on décide de tirer indépendamment) en fonction des tirages de cette loi. Nous pensons qu'avec cette méthode, l'estimation obtenue sur la seconde base de données aurait déjà plus de chances d'appartenir à l'ensemble des valeurs prises par la perte totale assurée. L'estimation d'une région de confiance dépendrait ensuite directement de la loi que l'on s'est donné.

3) Tester les deux cas extrêmes : une seule sous-garantie par police et toutes les garanties par police. Ainsi, on obtiendrait la borne supérieure et la borne inférieure de la perte totale assurée. Cet intervalle permettrait de connaître l'estimation maximum et l'estimation minimum de la perte bicentenaire qu'il nous est possible de faire sur le portefeuille A.

Cet exercice nous a permis de nous familiariser avec le modèle interne qui reposait alors sur le scénario cloud déterministe. Cette tache nous a en particulier sensibilisé à l'importance de la qualité des données et la nécessité pour l'actuaire de savoir fournir une estimation même en l'absence de variables à priori primordiales pour son calcul. Au cours de cet exercice, nous avons parfois été contraints d'utiliser des modèles imparfaits dont les hypothèses n'étaient pas toujours valides. Nous avons critiqués nos résultats et présenté leurs sources d'incertitude. Nous avons aussi constaté toute l'influence qu'avait la répartition des sous-garanties lors de l'application d'un scénario catastrophe.

2.3 Un scénario externe : Bashe Attack

Dans cette partie, nous présentons un scénario ransomware développé en externe. Ce scénario repose sur l'étude 'Bashe Attack Global infection by contagious malware' [11] produite dans le cadre du projet Cyber Risk Management (CyRim). Ce dernier est dirigé par Nanyang Technological University – Insurance Risk and Finance Research Center (NTU-IRFRC) en collaboration avec des entreprises et des universités dont Cambridge Center for Risk Studies. Ce projet a été financé par Aon Center for Innovation and Analytics, Lloyd's of London, MSIG, SCOR et TransRe.
Dans cette étude est décrite la 'Bashe attack' imaginée par le CCRS (the University of Cambridge Centre for Risk Studies). Cette attaque fictive décrit les impacts d'une cyber-attaque mondiale reposant sur un malware. Cet évènement jugé peu probable par l'étude est tout de même plausible et permet aux divers acteurs de l'économie d'évaluer les possibles conséquences d'un évènement d'une telle ampleur.

Ce scénario nous permet de comparer une modélisation externe provenant d'acteurs reconnus avec les modélisations internes d'AXA. Malgré une divergence dans les scénarios et les garanties touchées, il demeure intéressant de comparer l'ordre de grandeur de la perte totale engendrée par les modèles développés en interne et celle induite par le scénario CyRim, tant au niveau de la perte par évènement moyenne que des quantiles extrêmes.

Nous allons d'abord expliquer et synthétiser le plus clairement possible le scénario ransomware développé par l'étude CyRim. Nous invitons le lecteur à consulter l'étude complète pour tout détail

complémentaire. Nous justifierons ensuite nos choix de modélisation lorsque l'utilisation d'un paramètre n'est pas clairement spécifiée par l'étude ou bien que nos données ne nous permettent pas de suivre la mise en œuvre recommandée.

2.3.1 Introduction au scénario

Nous décrivons d'abord le principe de l'attaque avant de nous intéresser à la modélisation.

2.3.1.1 Principe de l'attaque

Un groupe de hackers développe un ransomware afin d'infecter le plus d'entreprises possible. Ce virus se répand via des emails dont le titre est 'Year-End-Bonus'. Une pièce jointe appelée 'BonusScheme.pdf' déclenche le virus. Le rôle clé du *Social Engineering* dans la propagation du virus est ici mis en valeur. Lorsque la pièce jointe est ouverte, le ransomware est téléchargé et exécuté en tâche cachée. Quelques minutes après l'ouverture du fichier, toutes les données stockées sur les ordinateurs et serveurs reliés sont encryptées. Un écran noir apparait, demandant à la victime de payer une rançon de 700USD$ pour décrypter les données. Pour poursuivre sa propagation, le virus envoie un mail similaire à tout le répertoire de contacts de la victime.
Des pertes considérables sont imputées à l'économie mondiale.

2.3.1.2 Les variantes de l'attaque

Dans l'étude, trois variantes d'attaque sont présentées. Il est précisé que chacune de ces variantes constitue une attaque peu probable mais ayant un fort impact.
La première variante nommée S1 est susceptible de toucher 43,10% des systèmes informatiques mondiaux. CyRim juge que les hypothèses utilisées dans ce scénario représentent le « Best Estimate » d'une attaque Ransomware mondiale.
La seconde nommée S2 représente des hypothèses plus sévères quant à l'impact de l'attaque. Cette attaque peut toucher 99% des systèmes informatiques.
La dernière nommée X1 présente un scénario jugé encore plus extrême, et est supposé homogène à un quantile à 95% de la perte par évènement. Dans ce cas, le ransomware est de type *wiper* détruisant les données des ordinateurs contaminés.
Les variantes S1, S2 et X1 diffèrent les unes des autres par la sévérité des valeurs numériques de leurs paramètres ainsi que le type de perte générée : contrairement à X1, S1 et S2 ne causent pas de frais de reconstitution de données et de logiciels.

Le schéma ci-dessous présente le déroulement du scénario ransomware de CyRim :

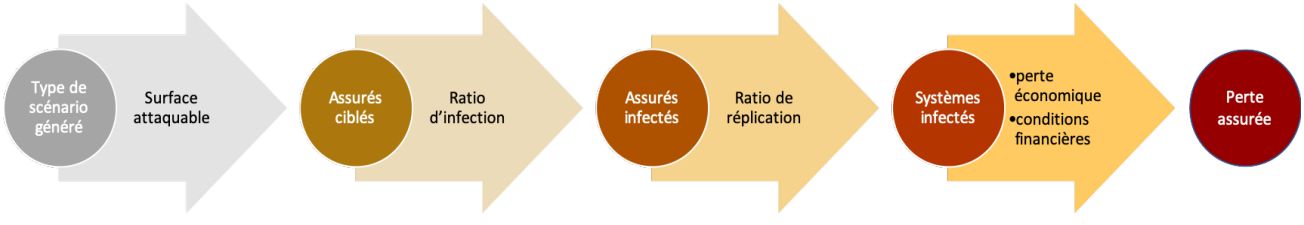


Figure 10-Schéma du déroulé de l'attaque Bashe

Conditionnellement à la variante d'attaque choisie :
1. La **surface d'attaque** est déterminée. Cette surface d'attaque représente l'ensemble des systèmes informatiques vulnérables au ransomware.
2. Le **ratio d'infection,** donne ensuite la proportion d'entreprises impactées par l'attaque. Il représente en quelque sorte la capacité du ransomware à se propager dans l'économie.
3. Enfin, le **ratio de réplication,** définit le degré de sévérité de la perte des entreprises réellement impactées. Il représente la capacité destructrice du ransomware lorsqu'il touche une entreprise.
4. Les pertes économiques sont calculées en fonction du scénario et du ratio de réplication impactant chaque entreprise touchée. Les conditions des contrats sont appliquées pour obtenir la perte assurée.
On comprend donc ici que les 3 variantes d'attaques se distinguent tant par leur portée que par leur sévérité.

2.3.1.3 Les pertes envisagées par CyRim

Il est intéressant d'étudier l'ordre de grandeur des pertes produites par chacune des variantes d'attaque. L'étude CyRim fournit une estimation de ces pertes que nous présentons dans le tableau suivant :

	S1	S2	X1
Number of infected global companies	250,000	501,000	613,000
Total direct economic loss	$59	$110	$133
Productivity and consumption loss	$50	$93	$112
Clean-up loss	$8	$15	$18
Cyber extortion loss	$1	$2	$2
Total indirect economic loss	$26	$49	$60
Total global economic loss	$85	$159	$193

Tableau 15-Pertes par variante de l'attaque

On note que l'attaque la moins sévère, S1, cause des dégâts 8 fois supérieurs à NotPetya. Les variantes S2 et X1 sont encore plus sévères, avec une perte 16 fois supérieure à NotPetya pour S2 et 19 fois pour X1. Les pertes économiques sont divisées en pertes directes (perte d'exploitation, frais de nettoyage et remplacement des systèmes informatiques, coût des rançons) et indirectes (perte d'exploitation contingente). Les scénarios établis par CyRim représentent donc un ransomware sans précédent et reflète les craintes suscitées par le marché de l'assurance cyber.

2.3.2 Les données de l'étude et nos choix de modélisation

En annexe de son étude, CyRim fournit un certain nombre de tableaux de données qui nous permettent d'appliquer le scénario ransomware à notre portefeuille d'assurés. Nous présentons un par un les tableaux de données que nous avons utilisés pour construire notre distribution de la perte assurée. Nous explicitons et justifions au fur et à mesure les hypothèses faites pour appliquer le scénario à notre portefeuille.
Il est important de noter que l'étude présente uniquement une manière de calculer la perte moyenne espérée pour chaque variante des scénarios. Dans un premier temps, la perte devrait être calculée pour chaque assuré. Ensuite, les coefficients fournis dans chacune des tables de surface attaquée par scénario, de taux d'infection et de taux de réplication sont censés être appliquées à chaque entreprise afin

d'obtenir la perte moyenne espérée. Cette manière de procéder ne permet pas d'évaluer la variation de la perte liée à la structure de notre portefeuille d'assurés. Afin d'étudier la distribution de la perte en cas d'évènement, nous avons choisi de générer aléatoirement le type d'attaque et de titrer aléatoirement les polices touchées ainsi que les coefficients de sévérité impactant chaque police.

2.3.2.1 Générateur d'attaques

Nous devons dans un premier temps tirer aléatoirement le type d'attaque simulée. Pour cela, nous avons besoin d'une distribution des évènements S1, S2 et X1. Cependant, aucune distribution de la fréquence des évènements n'est réellement fournie. Il est seulement spécifié que X1 correspond à une borne supérieure à 95% de la perte.

Hypothèse i) : Nous avons choisi d'affecter à X1 une probabilité de 5% et à S1 et S2 47.5% chacun.
Justification : Ce choix d'affectation des probabilités respecte l'unique hypothèse fournie par CyRim et reste assez conservateur. En effet, nous accordons le même poids à S1 et à S2 alors que S2 est décrit comme présentant des hypothèses plus sévères et donc supposées moins probables.

Le tableau suivant respecte l'hypothèse i) ainsi que la surface d'attaque fournie par CyRim à la page 19 de son étude.

Scenario	Attack Probability	Attack Surface
S1	0,475	43,10%
S2	0,475	97,30%
X1	0,050	97,30%

Tableau 16-Générateur d'attaques

Une fois le type d'attaque généré, nous devons déterminer la surface d'attaque.

Hypothèse ii) : La surface d'attaque est générée de façon purement aléatoire, c'est-à-dire sans information à priori sur la structure des entreprises touchées. Un assuré représente un type de système informatique.
Justification **:** L'étude ne détaille pas non plus comment est déterminée précisément la surface d'attaque initiale, mais elle présente tout de même A et B comme étant 2 systèmes informatiques bien distincts influant sur la surface d'attaque. Pour S1, seul le système A est vulnérable tandis que pour S2 et X1, B est lui aussi vulnérable. Nous ne connaissons pas la nature précise du système évoqué et ne disposant d'aucune information sur les systèmes informatiques présents dans notre portefeuille d'assurés, nous tirons directement un nombre d'entreprises en fonction du scénario tiré.

Hypothèse iii) : L'attaque touche l'économie mondiale et notre portefeuille de la même manière.
Justification : Aucune information ne suggère que notre portefeuille soit plus ou moins vulnérable que l'économie mondiale.

Nous utilisons un tirage discret induit par la colonne 'Attack Probability' du tableau Générateur d'attaque pour tirer S1, S2 ou X1. Selon le type d'attaque généré, la colonne 'Attack Surface' nous permet de sélectionner aléatoirement les polices attaquables. Nous obtenons donc les assurés ciblés par le ransomware.
A ce stade, nous sommes en mesure de tirer aléatoirement un type d'attaque et la surface attaquable.

2.3.2.2 Ratio d'infection

Disposant des entreprises vulnérables au ransomware, nous devons maintenant déterminer celles qui sont effectivement victimes d'une attaque. CyRim fournit pour chacun des scénarios une table donnant par secteur et par taille d'entreprise le pourcentage d'entreprises réellement infectées. A chaque secteur est associé un score de vulnérabilité (Sector Vulnerability Score : SVS), qui servira par la suite à déterminer le ratio de réplication.

Ci-dessous le tableau utilisé par CyRim pour affecter à chaque entreprise une taille catégorielle. Nous gardons la même segmentation. Ce tableau est disponible à la page 19 de l'étude.

Company size	Min number employee	Min revenue (dollars)
Premier	2 000	3 000 000 000
Large	500	40 000 000
Medium	100	10 000 000
Small	20	2 000 000

Tableau 17-Catégories de taille d'entreprises

Nous présentons ci-dessous le tableau donnant le pourcentage d'entreprises infectées pour le scénario S1 :

Sector	SVS	Premier	Large	Medium	Small
Business & Professional Services	3	4,00%	3%	3%	4%
Defense / Military Contractor	1	3,00%	3%	3%	2%
Education	5	9,00%	6%	6%	8%
Energy	2	5,00%	2%	2%	3%
Entertainment & Media	4	7,00%	4%	4%	5%
Finance - Banking	5	7,00%	6%	6%	8%
Finance - Insurance	4	6,00%	4%	4%	5%
Finance - Investment Management	4	6,00%	4%	4%	5%
Food & Agriculture	2	3,00%	2%	2%	3%
Healthcare	4	6,00%	4%	4%	5%
IT - Hardware	4	7,00%	4%	4%	5%
IT - Services	4	7,00%	4%	4%	5%
IT - Software	4	5,00%	4%	4%	5%
Manufacturing	4	5,00%	4%	4%	5%
Mining & Primary Industries	1	5,00%	1%	1%	2%
Pharmaceuticals	1	4,00%	3%	1%	2%
RealEstate/Property/Construction	4	6,00%	4%	4%	5%
Retail	5	8,00%	6%	6%	8%
Telecommunications	2	4,00%	3%	2%	3%
Tourism & Hospitality	3	5,00%	3%	3%	4%
Transportation/Aviation/ Aerospace	4	5,00%	4%	4%	5%
Utilities	2	4,00%	2%	2%	3%

Tableau 18-Ratios d'infection par Secteur et taille d'entreprise pour S1

Par exemple, parmi les entreprises vulnérables obtenues à l'étape précédente, au sein du secteur de l'énergie, 5% des entreprises de type 'Premier' seront effectivement impactées tandis que 2% des 'Large', 'Medium' et Small' seront touchées. Les Sector Vulnerability Scores (SVS) seront utilisés pour la suite du déroulement de l'attaque. CyRim ne communique pas sur la manière dont sont calculés ces scores. En annexe B sont disponibles les tableaux similaires pour les scénarios S2 et X1. Ces tableaux sont aussi disponibles en annexe de l'étude CyRim et n'ont pas été modifiés pour notre modélisation.
Nous appliquons encore une fois l'hypothèse iii) suggérant que notre portefeuille d'assurés se comporte de la même manière que l'économie mondiale.

Pour chaque secteur et taille, nous tirons parmi la surface attaquable un certain nombre d'entreprises en prenant soin de respecter le tableau des ratios d'infection du scénario.
A ce stade nous avons à notre disposition les entreprises touchées par l'attaque.

2.3.2.3 Ratio de réplication

Disposant des entreprises victimes du ransomware, nous devons à présent déterminer la sévérité avec laquelle est touchée chaque victime. Le ratio de réplication permet de modéliser ce degré de sévérité. Dans l'étude, une distribution discrète est fournie. Nous avons pris la liberté de nommer $R_i i=1…5$ les cinq degrés croissants de ratios de réplication, dont la distribution est conditionnelle au score de vulnérabilité (SVS) du secteur de l'entreprise.
Ci-dessous la distribution proposée par CyRim et que nous avons suivie pour notre modélisation :

SVS	R_1	R_2	R_3	R_4	R_5
1	0,35	0,45	0,1	0,07	0,03
2	0,30	0,42	0,1	0,12	0,06
3	0,25	0,39	0,1	0,17	0,09
4	0,20	0,36	0,1	0,22	0,12
5	0,15	0,33	0,1	0,27	0,15

Tableau 19-Distribution des ratios de réplication

Hypothèse iv) : L'étude fournit des intervalles pour les valeurs prises par chaque R_i. Nous choisissons d'affecter le milieu de ces intervalles à chaque R_i sauf R_5
Justification : Aucune distribution au sein de ces intervalles n'est fournie. Nous choisissons de prendre une valeur fixe pour chaque R_i pour ne pas complexifier le modèle. Prendre le milieu de l'intervalle est un choix neutre.
Les valeurs des ratios de réplication sont renseignées dans le tableau suivant :

Ratio	Valeur
R_1	0,05
R_2	0,15
R_3	0,25
R_4	0,35
R_5	0,70

Tableau 20 - Valeurs des ratios de réplication

Pour chaque entreprise, le ratio de réplication est obtenu par un tirage aléatoire, conditionnellement au SVS de l'entreprise.
A ce stade nous connaissons pour chaque entreprise touchée le ratio de réplication qui lui correspond.

2.3.2.4 Pertes économiques

L'annexe de l'étude permet de calculer les pertes brutes correspondant à chaque couverture.

- Business Interruption (BI) : Le ratio de réplication détermine une durée totale d'altération de l'activité. Chaque jour altéré fait perdre à l'assuré un certain pourcentage de son chiffre d'affaires journalier. Ci-dessous le tableau présentant le pourcentage du chiffre d'affaire perdu en fonction de la durée d'interruption et du ratio de réplication.

Jours	R_1	R_2	R_3	R_4	R_5
5	5,00%	15,00%	25,00%	35,00%	50,00%
10	3,00%	9,00%	18,00%	28,00%	45,00%
15	1,00%	5,00%	9,00%	14,00%	23,00%
20	1,00%	2,00%	4,00%	7,00%	11,00%
25	0,00%	1,00%	2,00%	4,00%	6,00%
30	0,00%	1,00%	1,00%	2,00%	3,00%

Tableau 21-Pourcentage de chiffre d'affaires perdu en fonction de la durée d'interruption en jours et du ratio de réplication

Par exemple, pour une entreprise de YUSD$ chiffre d'affaires journalier affectée par un ratio R_1, la perte due à l'interruption d'activité sera :
$Perte\ brute_{BI} = Y \times [5 \times 5\% + (10-5) \times 3\% + (15-10) \times 1\% + (20-15) \times 1\%]$

- Cyber Extortion (CRE) : L'étude fournit un nombre moyen d'appareils informatiques par taille d'entreprise (Tableau 22). Le ratio de réplication multiplié par le nombre d'appareils informatiques donne le nombre d'appareils touchés. Il est écrit que 4% des appareils infectés sont décryptés en payant la rançon estimée à 700 USD$. On rappelle que pour WannaCry, la rançon était comprise entre 300 et 600 USD$.

- Incident Response Cost (IRC) : Les 96% restant des appareils infectés doivent être nettoyés. Ce coût est estimé à 350 USD$ par appareil touché.

- Data and Software Loss (CYL) : Cette garantie est touchée uniquement pour la variante X1 du ransomware, qui est alors un ransomware *wiper* qui efface les données des appareils contaminés. L'étude suppose que 5 ordinateurs clés par entreprise sont restaurés mais ne spécifie pas le coût de réinstallation des ordinateurs restants. Chaque ordinateur clé coute 500 USD$ à être restauré. Deux options sont donc envisageables : considérer uniquement le coût des 5 ordinateurs clés ou trouver une relation permettant d'étendre ce coût aux autres ordinateurs.
Hypothèse v) : Nous supposons la relation de proportionnalité suivante : 5 ordinateurs sont nécessaires pour restaurer les données et les logiciels non récupérés de 180 appareils. Il faut donc 25 ordinateurs pour en restaurer 900 et ainsi de suite.
Justification : Il ne nous semble pas envisageable que le coût soit le même pour une entreprise 'Small' et une entreprise 'Large' dont le nombre de données et de logiciels est plus important. Nous sommes conscients que le coût marginal d'un ordinateur à restaurer est sans doute décroissant, avec un effet de seuil lorsque l'ajout d'un ordinateur supplémentaire nécessite la restauration d'un nouvel ordinateur clé, par souci de rapidité. Supposer une relation linéaire n'est donc pas totalement aberrant. De plus, dans le cas de notre relation de proportionnalité, le coût est limité par :

$R_5 \times 500 \times 5 \times \frac{9000}{180} = 87\ 500\ USD\$$, tandis que si on considère uniquement 5 ordinateurs clés au total, le coût est limité à $R_5 \times 500 \times 5 = 1\ 750\ USD\$$ ce qui nous semble très faible pour une entreprise 'Premier'.

Le tableau suivant fournit les pertes incombant aux garanties CRE, IRC et CYL, avant application du ratio de réplication.

Size	Average number of devices	CRE_before_rep_rate USD$	IRC_before_rep_rate USD$	CYL_before_rep_rate USD$
Small	180	5 040	60 480	2 500
Medium	900	25 200	302 400	12 500
Large	3 750	105 000	1 260 000	52 083,33
Premier	9 000	252 000	3 024 000	125 000

Tableau 22-Pertes CRE, IRC, CYL avant l'application du ratio de réplication

Par exemple, pour une entreprise touchée de taille 'Medium' dont le ratio de réplication est R_3, les pertes seront :

$$Perte\ brute_{CRE} = R_3 \times 900 \times 4\% \times 700 = 0.25 \times 25\ 200 = 6\ 300\ \text{USD\$}$$
$$Perte\ brute_{IRC} = R_3 \times 900 \times 96\% \times 350 = 0.25 \times 302\ 400 = 75\ 600\ \text{USD\$}$$
$$Perte\ brute_{CYL} = R_3 \times 900 \times 500 \times 5 \times \frac{900}{180} = 0.25 \times 12\ 500 = 3\ 125\ \text{USD\$}$$

- Contingent Business Interruption (CBI): cette garantie est activée pour les entreprises non impactées directement par l'attaque. Parmi les entreprises non touchées directement par le ransomware, 46% des entreprises qui ont souscrit à la garantie CBI sont touchées, avec six degrés de sévérité différents dépendant de la durée de l'impact.
Ci-dessous le tableau permettant de calculer la perte brute associée au CBI :

Days	Companies impacted	Daily revenue lost
2,5	18%	45%
7,5	14%	32%
12,5	7%	16%
17,5	4%	8%
22,5	2%	4%
27,5	1%	2%

Tableau 23- Pertes CBI

Par exemple, pour une entreprise de Y USD$ chiffre d'affaires journalier et non impactée directement par le ransomware, la probabilité de ne contracter aucune interruption d'activité contingente est de 54% tandis que la probabilité de subir une interruption d'activité de 2 jours et demi est de 18%, de 7 jours et demi 14%, de 12 jours et demi 7% etc.
La perte en cas d'interruption d'activité de 7,5 jours est :

$$Perte\ brute_{CBI} = Y \times [\ 2.5 \times 45\% + (7.5 - 2.5) \times 32\%\ ] = 2.725 \times Y\ \text{USD\$}$$

2.3.2.5 Pertes assurées

Nous avons maintenant les pertes brutes par couverture auxquelles nous appliquons les conditions d'assurance, c'est-à-dire la priorité, le déductible, et la limite. Pour chaque sous-garantie :
$Perte\ assurée\ = min(\ limite - déductible; (Perte\ brute - \ priorité\ -\ déductible)_+)$

2.3.2.6 Stratégie d'implémentation

On organise le code de la façon suivante :
1) On calcule et on stocke tout d'abord chaque perte possible que peut subir un assuré. C'est-à-dire que pour chaque ratio d'infection, la perte imputable à l'assuré est calculée. Ainsi, un même calcul ne risque pas d'être fait en double lorsque le nombre de simulations augmente.
2) On simule un vecteur de 10 000 scénarios parmi S1, S2, X1
3) Pour chaque scénario tiré :
- on tire la surface attaquable
- on sélectionne aléatoirement les entreprises touchées parmi la surface (ratio d'infection)
- parmi les entreprises touchées, on assigne aléatoirement une sévérité (ratio de réplication)
- on assigne la perte économique calculée à l'étape 1 qui dépend du scénario et de la sévérité tirées
- on applique les conditions d'assurance (limite, déductible, priorité) afin d'obtenir la perte assurancielle.
4) On calcule la moyenne et le quantile à 99.5% de la perte assurée.

2.3.3 Application numérique : perte par évènement

Nous allons maintenant effectuer 10 000 simulations de l'attaque Bashe que nous venons d'adapter. La distribution ainsi obtenue sera la perte par évènement.

Dans notre cadre d'étude, le Destruction Rate (DR) correspond à la perte totale liée au contrats *affirmative First Party* divisée par l'exposition totale relative à ces mêmes contrats. Il est donc équivalent d'étudier la perte ou le Destruction Rate à une constante multiplicative près. L'exposition totale est calculée en sommant pour chaque police la GCV (Gross Cover Value) des contrats cyber *affirmative First Party* définie par :

$$GCV = (limite\ de\ couverture - déductible\ de\ couverte) \times share$$

Dans un premier temps, on s'intéressera à la convergence du DR moyen. Puis on regardera son quantile à 99.5% avant de nous intéresser à la répartition moyenne de la perte par couverture.

2.3.3.1 Perte moyenne par évènement

Par Monte Carlo nous obtenons le DR moyen par évènement muni de son intervalle de confiance à 95% construit à l'aide du Théorème Central Limite (TCL) et du lemme de Slutsky (rappelés en annexe). Voici le graphique donnant la convergence de l'estimateur :

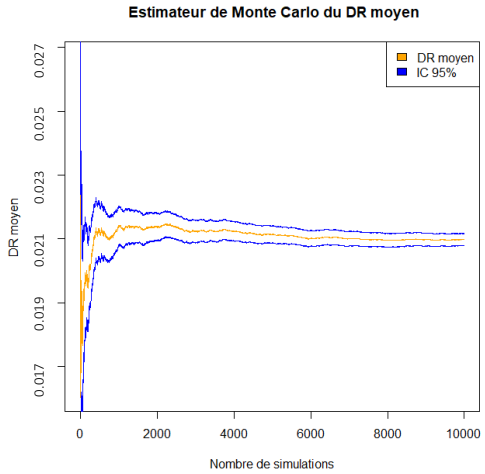


Figure 11-Estimateur de Monte Carlo du DR moyen en cas d'évènement

L'estimateur est plat, ce qui montre la convergence pour 10 000 simulations.
Les résultats sont renseignés dans le tableau suivant :

Nombre de simulations	Borne Inf IC 95%	DRMoyen par Monte Carlo	Borne Sup 95%
10 000	2.11%	2.13%	2.15%

Tableau 24-Estimateur de Monte Carlo de la perte moyenne en cas d'évènement

2.3.3.2 Quantile à 99.5%

On trace maintenant l'évolution de l'estimateur du quantile empirique.

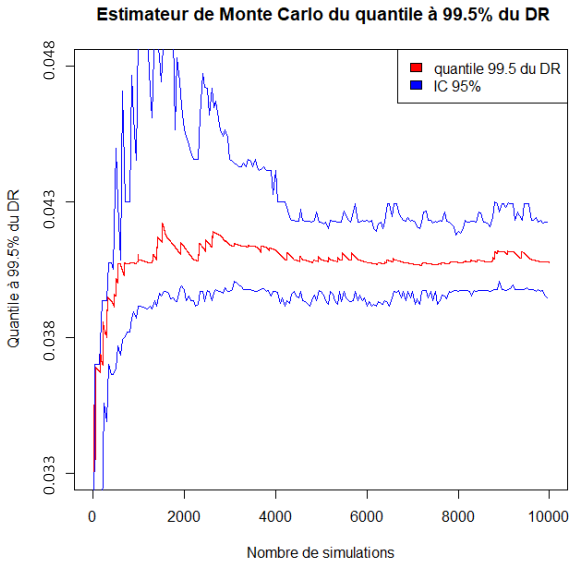


Figure 12-Convergence du quantile empirique à 99.5%

On a utilisé une approximation bootstrap générique pour avoir l'intervalle de confiance à 95% : pour chaque nombre N de simulation, on a tiré 1 000 échantillons bootstrap de taille N parmi les N premières simulations et on a calculé le quantile à 99.5%, on a ensuite pris pour chaque N les quantiles à 2.5% et

97.5% des quantiles à 99.5% qui ont été calculés. On obtient ainsi notre intervalle de confiance à confiance à 95% en fonction du nombre de simulations.

Nombre de simulations	Borne Inf IC 95%	Quantile 99.5% Monte Carlo	Borne Sup IC 95%
10 000	4.02%	4 .12%	4.22%

Figure 13-Estimateur de Monte Carlo de la perte à 99.5% en cas d'évènement

Après 10 000 simulations selon les 3 scénarios différents, la valeur du quantile empirique à 99.5% du DR est estimée 5.79%. On observe un pic de variation entre 9 000 et 10 000 simulations ce qui nous pousse à nous interroger sur la stabilité des résultats.

Pour s'assurer de la stabilité du quantile, on effectue 50 000 simulations :

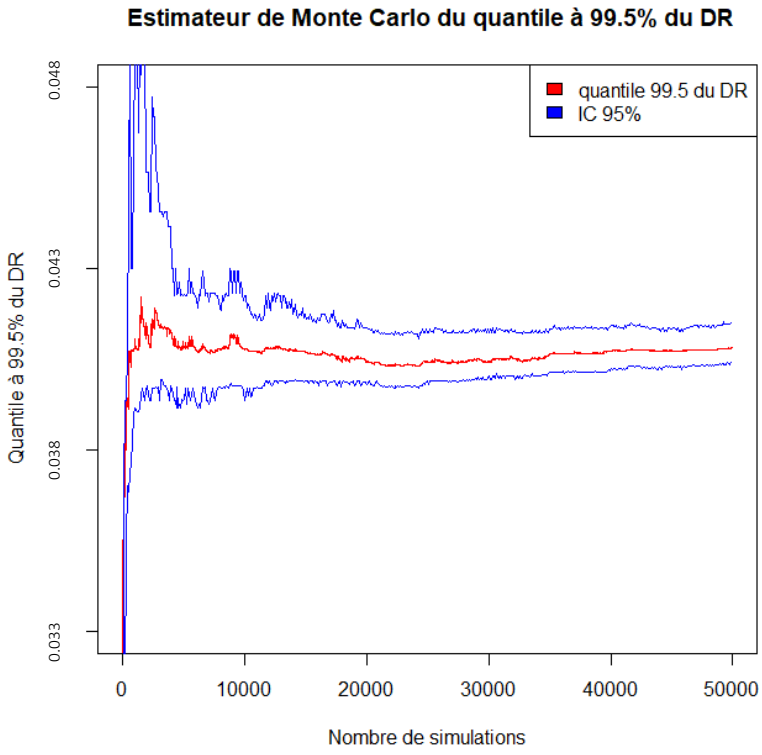


Figure 14 - Estimateur de Monte Carlo du quantile à 99.5% du DR avec 50 000 simulations

Nombre de simulations	Borne Inf IC 95%	Quantile 99.5% Monte Carlo	Borne Sup IC 95%
50 000	4.10%	4.13%	4.17%

Figure 15 - Estimateur de Monte Carlo de la perte à 99.5% en cas d'évènement

L'estimateur est quasi plat, ce qui atteste de la convergence de l'estimateur. Le quantile initial sur 10 000 simulations est proche de celui sur 50 000 simulations. Par rapport aux 10 000 simulations les 50 000 simulations ont tout de même permis de réduire l'amplitude de l'intervalle de confiance de

0.13%. Nous sommes donc satisfaits de ces résultats et conservons 4.13% comme valeur du quantile à 99.5%

2.3.3.3 Distribution des pertes en cas d'évènement

On trace ici la distribution u DR en cas d'évènement :

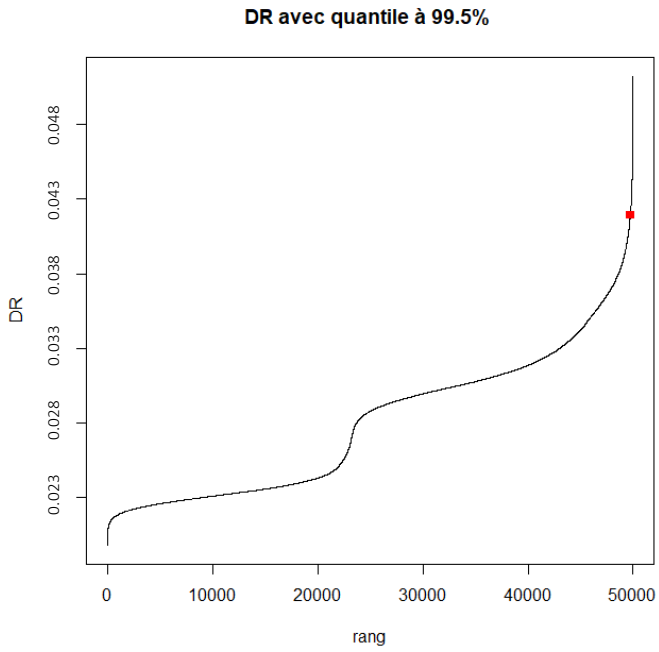


Figure 16 - Distribution du DR

On remarque un saut dans la fonction de perte autour de la 20 000ème perte, ce qui correspond à la zone de transition entre les pertes générées par une variante S1 et celles générées par une variante S2. En effet, on sait qu'on simule environ 4 750 pertes générées par une attaque de type S1 pour 10 000 simulations. Ce saut témoigne d'une disparité entre les pertes générées par S1 et celles générées par S2. Les valeurs communes des pertes induites par S1 et S2 sont peu fréquentes.

2.3.3.4 Répartition des pertes par sous-garanties

Rappelons que les scénarios S1, S2 et X1 sont classés du moins au plus sévère. On présente dans le tableau suivant les pertes moyennes par sous-garanties selon le scénario simulé :

Scenario	Perte moyenne BI (m USD$)	Perte moyenne CBI (m USD$)	Perte moyenne CRE (m USD$)	Perte moyenne CYL (m USD$)	Perte moyenne IRC (m USD$)
S1	40	136	1	0	3
S2	173	125	2	0	14
X1	249	121	3	35	21
All scénarios	114	130	1	2	9

Tableau 25-Pertes par sous-garanties selon les scénarios

On observe que le type de scénario influe de manière contraire sur BI et CBI : BI est croissant de la sévérité du scénario tandis que CBI est décroissant de la sévérité du scénario. Cela semble peu plausible pour une attaque réelle : on a plutôt tendance à penser qu'une victime directe engendre X victimes

indirectes. Lorsque le nombre de victimes augmente, le nombre de victimes collatérales augmente lui aussi. Cette incohérence s'explique par la manière dont est calculée la perte par sous-garanties : pour BI on tire un nombre plus grand d'entreprises victimes lorsque la sévérité de l'attaque est grande. Au contraire pour CBI, lorsque la sévérité de l'attaque est grande, on tire parmi un ensemble plus restreint les entreprises concernées par CBI.
Il est plus logique que toutes les pertes par sous-garanties augmentent quand la sévérité de l'attaque est plus importante.

2.3.4 Tests de sensibilité

On teste maintenant la sensibilité du modèle à ses paramètres. Pour comparer le modèle conditionnellement aux mêmes tirages, on teste la sensibilité aux paramètres en initiant les tirages à la même graine aléatoire dans R via la fonction « set.seed() » pour chaque variation d'un paramètre du modèle.
On effectue dans chaque cas 10 000 simulations. Par conséquent, on comparera nos résultats à la perte moyenne obtenue en 2.3.3.1) et au premier quantile trouvé en 2.3.3.2).

Nous pensons que la perte totale assurée est très dépendante du nombre de victimes. Par conséquent, pour les tests de sensibilité aux variables influant sur la portée de l'attaque (probabilité de S1, S2, X1 ou taille des surfaces d'attaque ou ratios d'infection) on s'attend à ce que la perte générée par le modèle soit sensible aux variations de ces paramètres. En effet, il est logique que la perte totale assurée soit très dépendante du nombre de victimes.
En revanche, la perte d'un individu étant bornée (par les limites et déductibles et attachement point dans les conditions du contrat) nous pensons que faire varier la perte au niveau de chaque assuré aura moins d'influence sur la perte totale. On s'attend donc à ce que les variables influant sur la sévérité d'une perte économique (ratio de réplication) fassent moins varier la perte générée par le modèle. Ceci est dû à la structure du portefeuille d'assurance qui est pourvu de limites. Par exemple en présence d'une limite faible, une très forte augmentation des pertes n'est pas totalement imputée au portefeuille.
Montrons quelques tests de sensibilité permettant de vérifier ces deux hypothèses.

2.3.4.1 Sensibilité au Nombre d'individus touchés

On teste ici la sensibilité à la surface d'attaque qui influe directement sur le nombre de victimes. On a effectué les chocs suivants sur le vecteur de surfaces d'attaque : -40% -20% + 2.7% tous égaux à 0.973

Surface Variation	Monte Carlo Mean Loss (USD$)	Mean Loss Variation	$\frac{Mean\ Loss\ Variation}{Surface\ Variation}$
0%	256 626 005	0,00%	-
-40%	209 093 872	-18.52%	46.30%
-20%	233 227 491	-9.12%	45.59%
2.70%	260 281 844	1.42%	52.76%
16.85%	281 815 753	9.82%	58.25%

Tableau 26 - Sensibilité à la surface d'attaque

Comme nous l'avions anticipé, la perte totale assurée sur notre portefeuille est très dépendante du nombre de victimes : une variation de 1% de la norme L^2 du vecteur de surfaces provoque une variation d'au moins 0.4% de la perte moyenne.
Nous pourrions plonger plus en détails et voir quelle variable influe le plus sur le nombre d'individus infectés.
On s'intéresse maintenant au quantile à 99.5% :

Surface Variation	Empirical quantile (USD$)	99.5% Quantile Variation	$\frac{Quantile\ Variation}{Surface\ Variation}$
0%	495 840 794	0%	-
-40%	383 444 772	-22.67%	56.67%
-20%	437 349 427	-11.80%	58.98%
2.70%	507 036 198	2.26%	83.62%
16.85%	498 483 823	0.53%	3.16%

Tableau 27 - Sensibilité au ratio de réplication

Ici aussi, on remarque que le quantile est très dépendant de la surface. On a 3 fois sur 4 un ratio de variation supérieur à 50%.
Les résultats du quatrième test présentés ainsi sont trompeurs : on pourrait penser qu'en augmentant la surface attaquée le ratio de variation devient faible. Mais ceci est en fait dû à la manière dont on a modifié le vecteur des surfaces attaquables : Nous avons égalisé toutes les surfaces à 97.3% pour réaliser ce test. Les surfaces d'attaque des scénarios S2 et X1 n'ont donc pas évolué par rapport au scénario classique. Le quantile étant issu de ces deux scénarios, on remarque alors une très faible variation du quantile. Les simulations issues de ce test pourraient permettre de regarder, à surface égale, l'influence des autres variables de sévérité telles que le ratio d'infection et de réplication.

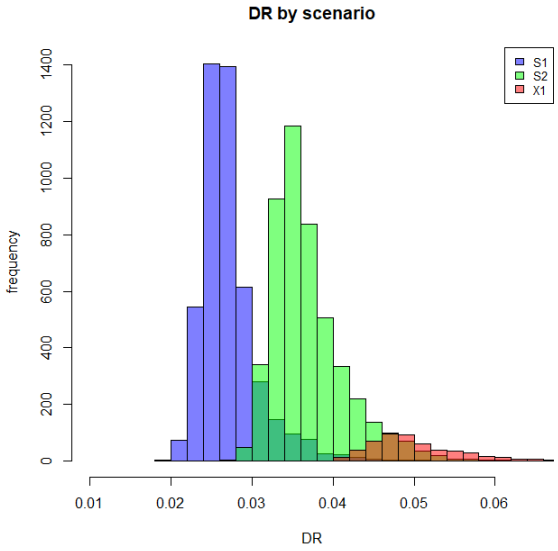


Figure 17 - DR par scénario à surface égale

La surface d'attaque n'est pas la seule variable influant sur le nombre de victimes : le ratio d'infection joue aussi un rôle important sur le nombre d'infectés. L'objectif était ici de démontrer que la perte générée par le modèle était sensible au nombre de victimes, nous ne ferons donc pas de tests sur les ratios d'infection.

2.3.4.2 Sévérité de la perte individuelle : ratios de réplication

Pour tester la sensibilité du modèle aux coûts individuels, on s'intéresse aux ratios de réplication. On décide de faire varier chacune des composantes du vecteur des ratios de réplication de -40%, -20%, +20%, +40%. Ainsi, la norme L^2 du vecteur des ratios de réplication est multipliée respectivement par 0.6, 0.8, 1.2, 1.4.
On s'assure que les ratios sont toujours compris entre zéro et un. On vérifie que plus particulièrement que le ratio le plus élevé R_5 est inférieur à un : $0.7 \times 1.4 = 0.98$

On s'intéresse dans un premier temps à la moyenne de la perte. Voici un tableau récapitulatif des résultats obtenus avec 10 000 simulations pour chaque vecteur de ratios de réplication :

Rep Rate Variation	Monte Carlo Mean Loss (USD$)	Mean Loss Variation	$\frac{\textit{Mean Loss Variation}}{\textit{Rep Rate Variation}}$
0%	256 626 005	0%	-
-40%	252 169 647	-1.74%	4.34%
-20%	254 444 347	-0.85%	4.25%
+20%	258 665 429	0.79%	3.97%
+40%	260 627 762	1.56%	3.90%

Tableau 28-Sensibilité de la perte moyenne aux ratios de réplication

On observe donc que le modèle n'est pas très sensible au vecteur de ratio de réplication puisque le ratio du pourcentage de variation de la perte moyenne divisé par le pourcentage de variation des ratios de réplication est toujours inférieur à 5%.
On rappelle que ce ratio représente la capacité destructrice du ransomware lorsqu'il touche une entreprise. Dans nos simulations, modifier ces ratios revient donc à conserver les mêmes entreprises touchées tout en modifiant leurs pertes. On peut donc penser que les limites des contrats sont assez faibles comparées aux pertes simulées, ainsi la perte totale assurée varie moins lorsqu'on augmente les pertes que lorsqu'on les diminue.

On s'intéresse maintenant au quantile à 99.5% :

Rep Rate Variation	Empirical quantile (USD$)	99.5% Quantile Variation	$\frac{Quantile\ Variation}{Rep\ Rate\ Variation}$
0%	495 840 794	0%	-
-40%	477 414 491	-3,72%	9,29%
-20%	486 211 266	-1,94%	9,71%
+20%	506 014 868	2,05%	10,26%
+40%	516 601 541	4,19%	10,47%

Tableau 29-Sensibilité du quantile à 99.5% aux ratios de réplication

Il faut garder à l'esprit que les résultats sont fournis pour 10 000 simulations ce qui n'est pas suffisant pour une estimation précise d'un quantile.
On observe tout de même que la sensibilité du quantile à 99.5% de la perte générée par le modèle semble un peu plus sensible aux ratios de réplication que la moyenne : les rapports $\frac{Quantile\ Variation}{Rep\ Rate\ Variation}$ dépassent tous 5%, mais restent tout de même largement inférieurs à 20%.

Ces résultats confirment nos premières intuitions : le modèle est peu sensible aux variables de sévérité lorsqu'il est appliqué à notre portefeuille. Des résultats différents peuvent être observés selon la structure des portefeuilles, ce qui souligne l'influence de la gestion de l'exposition dans les contrats d'assurance cyber.

2.3.5 Comparaison avec le scénario cloud

Pour comparer les résultats à notre scénario cloud, voici un d'abord un tableau récapitulatif de la répartition de la perte moyenne totale

Sous-garantie	% de la perte dans l'attaque Bashe	% de la perte dans le scenario Cloud
BI	44.5%	0%
CBI	50.6%	46%
CRE	0.6%	0%
CYL	0.7%	11%
IRC	3.6%	26%
RLD	0%	17%

Tableau 30-Comparaison des contributions des sous-garanties à la perte totale

Au vu de ces différences entre les pertes selon les scénarios, il est primordial pour l'assureur d'avoir un modèle illustrant différents types de menaces cyber. En effet, un modèle doté d'un seul scénario aura tendance à toucher toujours les mêmes garanties, ce qui ne signifie pas pour autant que les autres garanties ne comportent aucun risque, leur risque n'est simplement pas modélisé par le scénario en question. Notons tout de même que la garantie la plus touchée dans les deux scénarios est la garantie

BI (interruption d'activité). Dans le cas d'un ransomware ou d'une attaque de cloud, une part des systèmes informatiques des victimes est rendue indisponible. Ces choix de modélisation supposent une forte dépendance des assurés aux systèmes informatiques.

Le DR bicentenaire du scénario cloud est légèrement plus faible, mais du même ordre de grandeur que le celui renvoyé par l'attaque Bashe, ce qui conforte les hypothèses prises pour construire le scénario cloud. Les hypothèses conservatrices quant à la distribution des variantes d'attaques contribuent à renforcer la sévérité de l'attaque Bashe.

Conclusion

Dans ce second chapitre nous nous sommes familiarisés avec la structure du modèle d'accumulation cyber *affirmative First Party*. Nous avons expliqué brièvement en quoi consistait le scénario cloud et appliqué ce dernier pour calculer la perte bicentenaire relative à un portefeuille de coassurance. L'intégration de ce portefeuille nous a permis de souligner l'importance de la qualité des données lors de l'évaluation d'un risque. Nous avons montré l'influence de la répartition des sous-garanties lors du calcul de la perte assurée via l'application d'un scénario. L'implémentation de l'attaque Bashe, touchant des sous-garanties différentes, nous a permis de découvrir d'autres méthodes de construction d'un scénario d'accumulation. La perte bicentenaire renvoyée par l'attaque Bashe n'est pas identique à celle renvoyée par le scénario cloud, mais l'ordre de grandeur est tout de même comparable, ce qui conforte donc les choix faits pour la construction du scénario cloud.
De ce chapitre, nous retiendrons donc que la répartition des sous-couvertures de notre portefeuille et le choix des sous-couvertures impactées par le scénario influencent fortement la perte assurée. Ces éléments motivent la mise en place d'un scénario supplémentaire pour compléter notre vision du risque porté par notre portefeuille.
.

Chapitre 3
Nouveau scénario : analogie entre cyber et pandémie

Dans ce chapitre nous allons construire un nouveau scénario stochastique à intégrer au modèle cyber. Pour ce faire, nous proposerons une analogie entre risque cyber et risque de pandémie et adapterons un modèle épidémiologique pour modéliser la propagation d'un virus informatique au sein de notre portefeuille d'assurés. Nous justifierons dans un premier temps cette analogie avant de présenter quelques modèles épidémiologiques simples : les modèles compartimentaux déterministes. Nous établirons ensuite la structure de notre modèle cyber malware avant de détailler le scénario que nous allons construire : une attaque ransomware. Nous expliquerons le fonctionnement de notre modèle statistique et justifierons le recours au cadre bayésien pour estimer les paramètres du modèle. Nous utiliserons la méthode Approximate Bayesian Computation (ABC) pour procéder à l'estimation des lois *a posteriori* des paramètres du modèle. Notons bien les deux étapes distinctes que sont l'estimation des lois *a posteriori* des paramètres du modèle puis la simulation d'évènements à partir de ces lois *a posteriori*. Nous utiliserons NotPetya comme référence pour estimer les lois de certains paramètres du modèle tandis que les simulations seront obtenues en nous affranchissant de certaines conditions spécifiques à NotPetya.

3.1 Les modèles épidémiologiques

Une pandémie est une épidémie touchant un grand nombre de personnes et dont l'étendue géographique n'est pas toujours maitrisable. C'est donc une maladie ou une infection qui contamine potentiellement plusieurs continents.

3.1.1 Choix d'une telle analogie

Plusieurs raisons nous incitent à proposer un parallèle entre la modélisation du risque de pandémie et du risque cyber. Dans la définition proposée ci-dessus, nous retrouvons tout d'abord le caractère contagieux et systémique du risque cyber. Notons qu'une pandémie se propage de régions en régions (via les réseaux de transports internationaux par exemple), ce qui n'est pas le cas pour un virus informatique dont la propagation peut être plus fulgurante et toucher en l'espace de quelques secondes des régions diamétralement opposées. Ces deux menaces ont donc une grande portée, avec un temps de propagation différent. Le caractère imprévisible est lui aussi commun aux deux risques. Malgré une veille de l'OMS sur les maladies susceptibles d'engendrer une pandémie, la version du virus qui engendrerait une pandémie n'existe à priori pas aujourd'hui. On souligne donc aussi le caractère évolutif du risque de pandémie qui, à l'image d'un hacker développant une nouvelle version d'un programme malveillant, évolue via des mécanismes de mutation comme le shift ou le drift [18]. Les deux risques sont dotés d'un caractère latent : qu'il s'agisse du virus informatique ou d'une maladie, une période d'incubation du virus peut être constatée.

Au vu du faible nombre de données disponibles concernant les évènements cyber d'accumulation reposant sur un virus informatique, nous souhaitons proposer un modèle simple pour illustrer cette analogie. Nous avons donc choisi d'étudier les modèles compartimentaux. Si le lecteur le souhaite, il peut consulter le chapitre 3 de la partie II du mémoire d'Actuariat de Monsieur Romain SPEISSER [19] qui explique les différents types de modèles épidémiologiques ainsi que leurs avantages et inconvénients.
Nous présenterons d'abord différents types de modèles épidémiologiques compartimentaux avant d'en choisir un que nous adaptons au risque cyber.

3.1.2 Quelques modèles épidémiologiques compartimentaux

Les modèles compartimentaux sont constitués de deux éléments : les compartiments et les règles.

Les compartiments divisent la population totale N exposée au risque dans différents états possibles liés à la maladie ou l'infection. Les principaux compartiments qui nous intéressent sont :
- S pour 'Susceptible', contient les individus n'ayant pas encore été infectés ou guéris. Ce compartiment est nécessaire pour toute modélisation.
- I pour 'Infected' ou 'Infectious', c'est-à-dire les individus ayant été contaminés par le virus. Ce compartiment est lui aussi nécessaire à toute modélisation et peut selon le type de maladie/infection être scindé en sous-compartiments afin de faire la distinction entre le degré d'infectiosité d'un individu infecté.
- E pour 'Exposed', contient les individus exposés au risque mais qui ne sont pas encore infectés. Ce compartiment permet de modéliser la période de latence entre le premier contact au virus et l'infection avérée.
- R pour 'Recovered', contient les individus ayant réussi à développer une immunisation contre la réinfection. Ou 'Removed', contient alors les individus retirés de la population (sans distinction entre mort et guérison).

D'autres compartiments permettant d'élargir le champs des possibles existent mais ne sont pas abordés dans ce mémoire :
- D pour 'Dead', contient les individus morts à la suite de l'infection
- Q pour 'Quarantine', contient les individus isolés de la population car ils sont porteurs de la maladie
- C pour 'Carrier', contient les individus porteurs de la maladie mais qui ne présentent pas de symptômes
- V pour 'Vaccinated', contient les individus vaccinés qui ne sont donc plus susceptibles d'être infectés et sont donc exclus de S.

Les règles, formulées à l'aide d'équations différentielles, définissent les conditions de passage d'un compartiment à un autre. Ces modèles peuvent être déterministes ou stochastiques.
Dans un cadre général, une fois infecté, un individu peut être envoyé vers les compartiments D, Q, C, R ou S selon les règles du modèle qui reflètent les caractéristiques du virus modélisé.

Présentons maintenant quelques modèles compartimentaux déterministes les plus classiques. Les solutions explicites sont données lorsqu'elles existent. Le lecteur peut trouver les résolutions des équations différentielles, lorsqu'une solution explicite existe, dans le chapitre 5 du mémoire d'Actuariat de Monsieur Kevin HADDAD [20].

Notations :
Soit $N(t)$ la population totale au temps t, avec $t \in [0;T]$. Pour tout compartiment $K \in \{ S, E, I, D, Q, R, V \}$, $K(t)$ désigne le nombre d'individus dans le compartiment K au temps t.

Une hypothèse classique en épidémiologie est de supposer la population fermée et constante, ce qui permet de simplifier la modélisation et les calculs. Nous supposerons donc que $\forall t, N(t) = N$. Le portefeuille AXA est suffisamment grand et diversifié pour représenter une portion de l'économie mondiale. Nous supposerons donc que les effets observés sur notre portefeuille s'applique à la population mondiale. Ainsi, supposer la population fermée et constante est raisonnable puisque notre portefeuille d'assurés est stable sur une année. Les modèles suivants sont présentés avec cette hypothèse de population fermée et constante.

3.1.2.1 Le modèle Susceptible, Infected (SI)

La répartition de la population entre les deux compartiments est régie par les équations différentielles suivantes : pour tout temps t,

$$\begin{cases} N(t) = S(t) + I(t) = N \\ \dfrac{dS(t)}{dt} = -rS(t)I(t) \\ \dfrac{dI(t)}{dt} = rS(t)I(t) \end{cases}$$

Développé par HAMER en 1906 [21], ce modèle permet de modéliser des maladies pour lesquelles aucune guérison n'est possible, comme par exemple la tuberculose. Il comprend deux compartiments : S et I.
Ce modèle dispose d'un unique paramètre r qui représente la probabilité qu'un individu susceptible soit infecté.

3.1.2.2 Le modèle Susceptible, Infected, Susceptible (SIS)

La répartition de la population entre les deux compartiments est régie par les équations suivantes : pour tout temps t,

$$\begin{cases} N(t) = S(t) + I(t) = N \\ \dfrac{dS(t)}{dt} = -rS(t)I(t) + \ g\ I(t) \\ \dfrac{dI(t)}{dt} = rS(t)I(t) \ - \ g\ I(t) \end{cases}$$

A l'inverse du modèle SI, le modèle SIS permet de décrire des maladies pour lesquelles il est possible de guérir et d'être à nouveau infecté car les individus ne développent pas d'immunité, il s'agit par exemple des rhumes ou gastro. Cela se traduit par l'ajout d'un autre compartiment S dans le modèle et donc d'un paramètre g représentant la probabilité de guérison des individus infectés.

3.1.2.3 Le modèle Susceptible, Infected, Removed (SIR)

Développé par Kemarck et Mc Kendrick au début du XXème siècle [22], ce modèle permet de décrire la dynamique des épidémies de peste ou de choléra, pour lesquelles la mort advient de manière

récurrente. Attention, R contient ici les individus qui sont retirés de la population infectée. Ces individus retirés sont soit guéris, soit décédés. Par rapport au modèle SIS, la guérison n'est plus modélisée par un retour au compartiment S, mais est matérialisé par le passage vers l'état R.

Donnons ici une version standard du modèle SIR qui suppose les hypothèses suivantes en plus de la population fermée et constante:
-la population est supposée homogène, c'est-à-dire qu'un même taux moyen de transmission de l'infection est appliqué à la totalité de la population
-la population est totalement mélangée, c'est-à-dire que n'importe quel infecté peut contaminer n'importe quel individu susceptible.
Sous ces hypothèses, la répartition de la population entre les deux compartiments est régie par les équations suivantes : pour tout temps t,

$$\begin{cases} N(t) = S(t) + I(t) + R(t) = N \\ \dfrac{dS(t)}{dt} = -\dfrac{\alpha I(t)}{N} S(t) \\ \dfrac{dI(t)}{dt} = \dfrac{\alpha I(t)}{N} S(t) - \beta I(t) \\ \dfrac{dR(t)}{dt} = \beta I(t) \end{cases}$$

Le paramètre α représente la probabilité qu'un individu susceptible soit infecté, tandis que β s'interprète comme la probabilité qu'un individu infecté soit retiré. $\frac{I(t)}{N}$ représente la proportion d'individus infectieux au temps t.

Un infecté est introduit dans la population initiale. Sous nos hypothèses d'homogénéité et de mélange de la population, à chaque pas de temps, nous avons $\frac{\alpha I(t)}{N} S(t)$ susceptibles qui sont infectés par le virus et rejoignent le compartiment I. Chaque individu dans S a donc le même pourcentage de chances $\frac{I(t)}{N}$ d'être en contact avec un individu infectieux (hypothèse de population totalement mélangée). Parmi ces $\frac{I(t)}{N} S(t)$ contacts entre infectieux et susceptibles, seule une proportion α de susceptibles sont infectés (hypothèse de population homogène). I voit donc sa population augmenter de $\frac{\alpha I(t)}{N} S(t)$ et diminuer d'une proportion β qui passe à l'état retiré. L'état retiré peut contenir les individus décédés, guéris où immunisés.

Le modèle présenté suppose l'homogénéité et le mélange total de la population. Pour modéliser une population hétérogène certaines pratiques consistent à scinder la population en différent groupes dotés chacun de probabilités spécifiques de transmission ou transfert d'un état à l'autre. Pour une population humaine, il est commun de scinder la population en classe d'âge.
Si la population n'est pas totalement mélangée, il est aussi possible de la scinder et modéliser des contacts sociaux dans chaque groupe grâce à des graphes de Bernoulli [23] . Soit $G = (N, p)$ un graphe de Bernoulli défini sur N sommets avec p la probabilité qu'un contact se réalise entre deux sommets i et j (où : $i \neq j$ et $i, j = 1 ... N$). Pour toute paire d'individus du graphe à N sommets, un contact social a lieu avec une probabilité p. On peut alors indexer p selon les groupes de population afin de refléter l'hétérogénéité de la population totale.

3.1.2.4 Le modèle Susceptible, Exposed, Infectious, Removed (SEIR)

Ce modèle peut être utilisé pour modéliser des maladies comme la grippe. Par rapport au modèle SIR, l'introduction du compartiment E permet de modéliser en temps de latence entre l'exposition et la possibilité de transmettre la maladie. On introduit donc les individus exposés au virus contenu dans le compartiment E. Ces individus ont été infectés par la maladie mais ne peuvent pas encore la transmettre. Pendant cette période d'incubation du virus, ils développent peu à peu les symptômes de la maladie et finissent par devenir infectieux. Ils vont alors dans le compartiment I où ils sont en mesure de transmettre la maladie à des susceptibles et restent infectieux jusqu'à leur guérison ou mort. Ils vont alors dans le compartiment R.
Sous les mêmes hypothèses que le modèle SIR standard, les individus migrent entre les compartiments selon les équations différentielles suivantes : pour tout temps t,

$$\begin{cases} \dfrac{dS(t)}{dt} = -\dfrac{\alpha I(t)}{N} S(t) \\ \dfrac{dE(t)}{dt} = \dfrac{\alpha I(t)}{N} S(t) \; - \beta E(t) \\ \dfrac{dI(t)}{dt} = \; \beta E(t) \; - \; \gamma I(t) \\ \dfrac{dR(t)}{dt} = \gamma I(t) \end{cases}$$

Un infecté est introduit dans la population initiale. A chaque pas de temps, une proportion $\frac{\alpha I(t)}{N}$ des susceptibles est exposée au virus et rejoint le compartiment E. E voit donc sa population augmenter de $\frac{\alpha I(t)}{N} S(t)$ et diminuer d'une proportion β qui passe à l'état infectieux. I voit sa population augmenter de $\beta E(t)$ et diminuer d'une proportion γ. Les $\gamma I(t)$ quittant le compartiment I sont retirés et vont donc dans R.
Le graphique suivant présente l'évolution de la population au sein des compartiments S, E, I, R pour une population initiale de $N = 10\,000$. Il a été obtenu en appliquant le schéma de discrétisation d'Euler aux équations différentielles du modèles. Les paramètres du modèle sont fixes et prennent les valeurs suivantes : $\alpha = 0.8$; $\beta = 0.2$; $\gamma = 0.2$

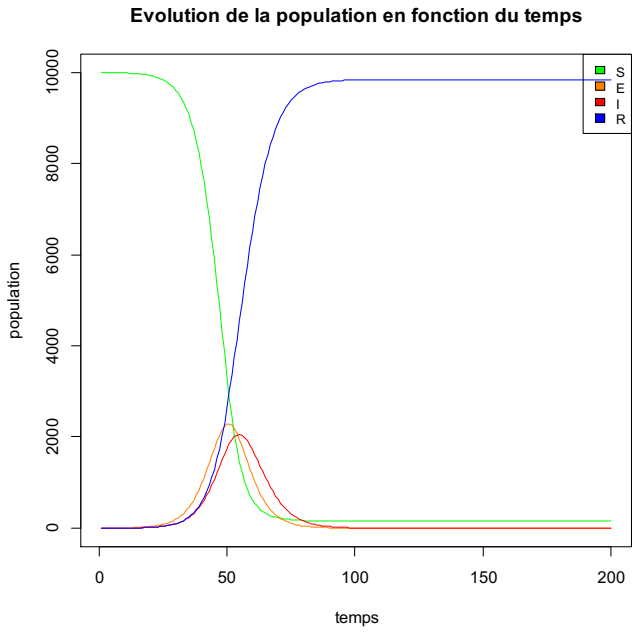


Figure 18-Evolution de la population dans le modèle SEIR

3.1.2.5 Remarques sur l'estimation des paramètres

Dans le cas d'un modèle déterministe, les taux de transfert d'un état à l'autre sont fixés et les malades restent dans chaque état de la maladie pendant des temps fixes. Par exemple, pour le modèle SEIR, les périodes latentes et d'infectieuses sont déterministes. Dans le cas d'un modèle stochastique, les taux de transmission du virus et les temps qui rythment l'état de santé d'une personne exposée sont rendus aléatoires.

Dans les deux cas précédents, les paramètres du modèle doivent être estimés grâce à des données. Pour la plupart des modèles, ces données sont issues d'observations de pandémies historiques relativement anciennes auxquelles sont parfois ajoutés des points fictifs. Ces points fictifs représentent souvent une catastrophe extrême susceptible de se produire dans un futur proche. Cet ajout permet d'incorporer aux données un évènement catastrophe (ou plusieurs) dont les caractéristiques sont adaptées à l'époque actuelle. Ainsi, les paramètres estimés prendront en compte les prévisions actuelles des caractéristiques d'une future pandémie.

L'estimation des modèles peut s'effectuer sur deux types de données :
-les processus complètement observés permettent d'estimer les paramètres du modèle en utilisant par exemple le maximum de vraisemblance
-les processus partiellement observés pour lesquels on ne dispose que d'informations partielles sur les temps infectieux, dates de contamination, rémission etc... Le modèle peut alors faire l'objet d'une estimation par la méthode E-M (Expectation-Maximisation), ou encore la méthode MCMC (Markov Chain Monte Carlo).

Conclusion : A ce stade, nous avons présenté quelques structures de modèles épidémiologiques et les caractéristiques de la population qui peuvent être prises en compte grâce aux hypothèses d'homogénéité et de mélange. Nous allons à présent construire le modèle.

3.2 Adaptation du modèle SIR

Pour bâtir notre scénario ransomware, nous souhaitons utiliser un modèle SIR pour simuler des victimes touchées par le virus. Ce modèle s'applique naturellement à la propagation d'un virus informatique : une population est initialement vulnérable au virus développé par un hacker. Ce dernier passe ensuite à l'attaque et réussi à infecter une partie de la population. La population infectée peut aussitôt transmettre le virus à d'autres individus tant qu'elle est reliée à des réseaux informatiques. Ce n'est que lorsqu'elle isole ses systèmes informatiques de tout autre réseau que la victime n'est plus infectieuse et peut commencer à réparer ses dégâts.
Nous allons dans un premier temps justifier plus en détails ce choix de compartiments avant de présenter le modèle malware et de décrire plus en détails le scénario ransomware.

3.2.1 Choix des compartiments

Parmi les modèles précédemment mentionnés, certains sont naturellement inadaptés.

Le modèle SI (susceptible infecté) ne permet aucune guérison possible. Or l'entreprise contaminée par le virus informatique ne reste pas infectée indéfiniment. Elle nettoie ses systèmes et les restaure voire les remplace si besoin. Le modèle SIS (susceptible infecté susceptible) suppose qu'une entreprise touchée pourra l'être une seconde fois. Ce schéma n'est pas réaliste pour le risque cyber : d'une part les victimes continuent souvent à réparer leurs dégâts après que l'attaque soit terminée, d'autre part une fois infectées par un virus (et conscientes de cette attaque) elles font le nécessaire pour sécuriser leurs systèmes contre ce type précis d'attaque subie.
Les modèles qui nous semblent le plus adéquats à notre problème sont le modèle SIR (susceptible infecté retiré) et le modèle SEIR (susceptible exposé infecté retiré). A première vue, nous sommes tentés par le modèle SEIR pour modéliser le temps de latence du risque cyber. Cependant, pour les maladies et virus touchant l'homme, ce temps de latence traduit l'impossibilité physiologique pour un malade de transmettre le virus. Pour un virus cyber dont l'objectif serait d'infecter le plus d'individus possible, on peut supposer qu'une fois un appareil infecté le code d'exécution de transmission du virus est automatiquement exécuté (c'était notamment le cas de NotPetya et WannaCry). De plus, pour le risque cyber le temps de latence fait plutôt référence à la période entre la contamination et le « Zero Day Vulnerability » qui correspond au premier jour où le virus est découvert et non pas le premier jour où il peut être transmis (une victime d'un spyware peut par exemple être infectée et avoir transmis le virus bien avant le moment où elle s'en rend compte). Cette divergence suggère de bannir le compartiment E.

Nous choisissons donc le modèle Susceptible, Infectés, Retiré (SIR) puisque ce modèle correspond à la dynamique de propagation d'un virus informatique.
On considère que S représente un groupe d'entreprises vulnérables à une certaine attaque dû à leurs profils informatiques. Le virus informatique infecte une première victime. Cette dernière a des contacts avec d'autres entreprises et transmet le virus avec une certaine probabilité.
Dès qu'une entreprise est touchée par le virus, elle est en mesure d'en contaminer une autre (via par exemple un échange de mail quasi instantané ou encore un serveur auxquels sont reliés en permanence d'autres susceptibles).
La durée pendant laquelle l'entreprise peut en infecter une autre sera modélisée par une variable aléatoire T_I de paramètre θ_I. Cette durée modélise le temps pendant lequel l'entreprise est encore reliée à de quelconques moyens de communication alors qu'elle est infectée. Une fois qu'elle a désactivé tous ses appareils contaminés (elle ne peut donc plus infecter personne), l'entreprise va dans le compartiment Retiré où elle va commencer à réparer les dégâts causés par l'attaque.
La durée correspondant à ce temps de réparation est modélisée par une variable aléatoire T_R de paramètre θ_R. Cette période, plus ou moins longue, influe sur les pertes économiques qu'essuiera l'entreprise une fois rétablie. Plus la période est longue, plus les pertes seront importantes.
On considère que l'entreprise fait le nécessaire pour ne pas être réinfectée par ce même virus (elle effectue par exemple une mise à jour ou restauration ou même remplacement de ses systèmes informatiques contaminés).
En parallèle de l'attaque, les services informatiques du monde entier tentent de déployer un patch pour corriger la faille exploitée. Une fois ce patch déployé, les entreprises ne pourront plus être contaminées par le virus. Ce temps nécessaire au déploiement d'un patch est modélisé par une variable aléatoire T_P de paramètre θ_P.
Une fois le patch déployé (ou la quelconque solution informatique trouvée), les Infectieux passent tous dans l'état Retiré et l'état Susceptible devient vide. Les entreprises Retirées commencent à réparer les dégâts causés par le virus pour une durée modélisée par T_R.

3.2.2 Présentation du modèle malware

Nous décidons de modéliser la propagation d'un virus exploitant une vulnérabilité présente dans un logiciel, un système d'exploitation ou un navigateur très répandu. Nous introduisons le modèle malware avant de nous concentrer sur le scénario ransomware.

Le schéma suivant introduit la structure du modèle malware que nous souhaitons mettre en place :

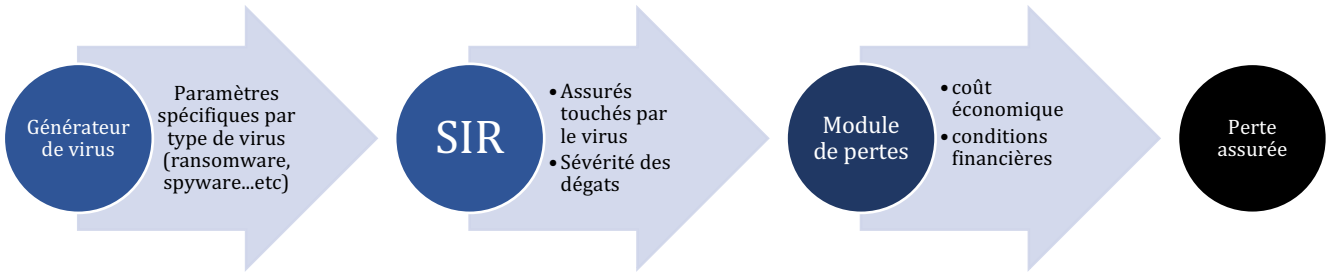


Figure 19 - Modèle Malware

Générateur de virus : produit les paramètres et hyper-paramètres propres à chaque attaque.
Le générateur de virus simule des types de malware. Chaque type de malware possède ensuite des paramètres spécifiques. Le SIR et le module de pertes sont donc simulés conditionnellement à ces paramètres spécifiques. Nous expliciterons plus en détails ces paramètres lorsque nous présenterons le scénario ransomware.

SIR : modèle stochastique qui génère des individus victimes et leurs caractéristiques.
Conditionnellement aux paramètres et hyper-paramètres donnés par le générateur, notre SIR adapté simule des entreprises infectées avec leurs temps infectieux et de réparation, les sévérités des dégâts et les caractéristiques de ces entreprises (comme leur secteur d'activité, leur chiffre d'affaires et leur pays).

Module perte : partie déterministe qui fournit un résumé de l'attaque.
Une fois les victimes simulées par le SIR adapté, on applique une fonction de coût économique h qui prend en entrée le type de malware, le temps infectieux et de réparation, les caractéristiques des victimes et renvoie un coût économique par type de sous-garantie.

Les paramètres du modèle SIR utilisés pour chaque type de virus sont différents. Par exemple, selon le type de virus, la propagation sera plus ou moins fulgurante et les pertes imputées aux entreprises ne seront pas de même type. Un spyware bien dissimulé a un temps infectieux plus long qu'un ransomware : en effet, le but du ransomware est de bloquer immédiatement l'activité informatique de la victime voire même d'endommager ses appareils et ses fichiers alors que le spyware a pour objectif de rester inaperçu et selon les cas de continuer à infecter d'autres victimes.
Les coûts sont aussi calculés différemment selon les types de malware. Les types de coûts résultants de ces deux catégories de virus ne sont pas non plus les mêmes : un ransomware cause principalement des pertes matérielles directes auxquelles s'ajoute le coût de la rançon alors qu'un spyware peut causer des

pertes de réputation (si des éléments compromettants sont divulgués sur l'assuré) ou de compétitivité (si des informations stratégiques sont dévoilées).

Pour chaque type de virus, l'estimation des paramètres peut être faite de manière indépendante. Dans ce mémoire, on se concentre uniquement sur l'estimation des paramètres du scénario ransomware. Les paramètres du scénario ransomware seront estimés à partir du ransomware le plus dévastateur jusqu'à présent : NotPetya.

3.2.3 Objectifs et obstacles à la construction du scénario ransomware

Nous souhaitons que le modèle ransomware repose sur des hypothèses différentes de celles du scénario cloud afin de compléter la vision du risque sur le portefeuille AXA. Nous voulons que le modèle permette de construire des évènements réalistes, proches d'attaques ransomware ayant déjà eu lieu, mais qu'il puisse aussi générer des évènements nouveaux et vraisemblables qui nous permettront d'obtenir une distribution de la perte assurée. Ces évènements nouveaux mais vraisemblables pourraient par exemple être une permutation différente des conditions de l'attaque, à savoir la durée totale, le système attaque ou le coût de la rançon. La structure du modèle devra aussi permettre d'intégrer des informations plus détaillées sur le profil informatique des assurés, informations qui seront obtenues dans un futur assez proche.

Dans l'idéal, nous souhaiterions utiliser des données réelles complètement observées pour estimer les paramètres du modèle SIR. Nous aurions besoin des informations suivantes :
- entreprises touchées,
- dates auxquelles ces entreprises sont infectées
- dates auxquelles ces entreprises ne sont plus infectieuses
- dates de début et fin des réparations
- liens et réseaux ayant amené un virus informatique à se propager

N'ayant pas accès à de telles données, nous devons trouver une solution pour estimer les paramètres du modèle. Donnons dès à présent les grandes lignes de notre procédure, qui sera expliquée plus en détails au fur et à mesure.
Nous allons construire un modèle statistique permettant de générer des entreprises infectées, leurs temps infectieux, leurs temps de réparation et la sévérité avec laquelle ces entreprises sont touchées. La construction d'une fonction de coût, que nous noterons h, associera à chaque victime un coût économique. L'idée sera ensuite d'estimer les paramètres du modèle permettant de générer des observations proche d'un évènement réel : NotPetya. Nous supposerons que les vraies observations (auxquelles nous n'avons pas accès) sont issues de notre modèle statistique et estimerons les paramètres du modèle tels que les observations générées soient proches de l'évènement réel. Cette notion de proximité entre l'évènement réel et nos simulations sera détaillée dans la suite du mémoire.

Dans la suite nous déciderons de nous placer dans un cadre bayésien qui permet de fournir une notion d'incertitude sur la valeur des paramètres du modèle, ceci passe par l'estimation de la loi *a posteriori* des paramètres.
Notons dès à présent qu'un modèle SIR classique ne fait pas intervenir la notion de coût économique mais permet uniquement de simuler des individus touchés et des temps de début et de fin de l'état infectieux. Dans notre cas, le coût interviendra dans la notion de proximité entre l'évènement réel et les observations générées. Nous verrons que les nombreuses informations sur les assurés influent sur le

coût et complexifient la vraisemblance du modèle, ce qui nous poussera à écarter la méthode classique d'estimation des modèles SIR, à savoir la méthode MCMC (Markov Chain Monte Carlo), et à choisir la méthode ABC (Approximate Bayesian Computation). Nous justifierons plus en détails ce choix au moment de présenter la méthode d'estimation de la loi *a posteriori* de nos paramètres.

3.2.4 Informations recensées sur NotPetya

Nous allons estimer notre modèle statistique à partir d'un évènement réel : NotPetya.
Nous donnons ici les informations que nous avons recensées sur NotPetya, son principe général ayant déjà été résumé dans le premier chapitre à la section 1.1.2.
NotPetya a touché plus de 2 000 entreprises dans le monde [24] pour un coût total de 10 milliards de dollars. Une autre attaque tout aussi connue, WannaCry, a touché 100 000 victimes pour un coût total de 8 milliards de USD$ [25]. Les rançon demandées par NotPetya et WannaCry n'ont été payées que par très peu de victimes [26] et leur coût variait entre 300 et 600 USD$.

Dans la première partie du mémoire nous avons évoqué la création d'une base de données recensant des évènements d'accumulation. Nous avons aussi construit une base spécifiquement dédiée à NotPetya. Donnons ici les éléments recensés concernant NotPetya.

Le tableau ci-dessous présente une liste non exhaustive de victimes de NotPetya. Pour ces victimes nous avons trouvé des informations qui nous aiderons à construire la fonction de coût du modèle, comme le secteur d'activité, le chiffre d'affaires annuel ou encore le nombre d'employés.

Entreprise	Secteur	Chiffre d'affaires (millions)	Devise	Nombre d'employés
Merck	Pharmaceutical	43 073	USD	69 000
FedEx	Transportation	69 200	USD	359 000
Saint Gobain	Manufacture	41 774	EUR	181 001
Maersk	Transportation	38 853	USD	80 220
Mondelez	Manufacture	29 600	USD	107 000
Reckitt	Manufacture	12 597	GBP	37 345
Renault	Automobile Manufacture	57 419	EUR	180 000
Auchan	Retail	50 986	EUR	358 914
SNCF	Transportation	31 681	EUR	203 865
Rosneft	Energy (oil gas)	126 781	USD	170 900
BNP Real Estate	Real Estate	811	EUR	351
WPP	Communication	15 602	GBP	134 281
DLA Piper	Legal services	2 440	USD	2 703

Tableau 31- Victimes de NotPetya et leur chiffre d'affaires et nombre d'employés (Source : Wikipedia)

Nous présentons dans le tableau 32 les pertes que nous avons recensées sur les victimes de NotPetya. Ces informations nous renseignent sur l'ordre de grandeur des pertes maximum pour une entreprise, mais ne sont pas à considérer comme un chiffre exact.

Entreprise	Perte (millions de dollars)	Source
DLA Piper	Environ 2,25	Sampson [27]
FedEx	Entre 400 and 300	Wired [28], Wavestone [29]
Maersk	300	Wired [28], Wavestone [29]
Merck	Entre 870 and 620	Wired [28], Wavestone [29]
Mondelez	188	Wired [28], Wavestone [29]
Reckitt	129	Wired [28], Wavestone [29]
Saint Gobain	Entre 384 and 250	Wired [28], Wavestone [29]

Tableau 32- Perte par entreprise pour NotPetya

On remarque que les 7 entreprises ci-dessus représentent à elles seules environ 2.2 milliards de dollars, soit 22% de la perte économique mondiale répartis entre moins de 0.35% des 2 000 entreprises touchées. Le reste des victimes se partage donc une perte de 7,8 milliards, soit en moyenne 3,91 millions de dollars (en supposant exactement 2 000 victimes au total). On remarque donc une grande amplitude de valeurs prises par le coût individuel et une faible proportion de pertes supérieures à 100 millions.
Nous présentons maintenant les temps de réparation trouvés lors de nos recherches :

Entreprise	Temps (jours)	Type	Source
DLA Piper	21	Réparations totales	itnews [30]
FedEx	84	Réparations totales	Les Echos [31]
Maersk	10	Activité partielle	Zdnet [32]
Maersk	23	Réparations totales	Les Echos [31]
Mondelez	36	Réparations totales	Les Echos [31]
Reckitt	14	Réparations totales	Les Echos [31]
Saint Gobain	13	Réparations totales	Les Echos [31]

Tableau 33 - Temps des réparations totales et de reprise de l'activité

Dans le tableau ci-dessus, on remarque deux types de temps communiqués : les temps correspondant à la fin des mesures prises en conséquence de l'attaque et la durée nécessaire avant la reprise normale de l'activité.
Maersk est la seule entreprise pour laquelle on dispose de ces deux temps. Dans l'article de Zdnet on apprend que Maersk a nécessité 10 jours avant de reprendre une activité normale, ce qui ne signifie pas pour autant que toutes les procédures de nettoyage et de mise en place d'une cyber sécurité plus robuste étaient terminées en 10 jours. Ces procédures ont nécessité un temps plus important (au minimum 23 jours).

Entreprise	Objets endommagés	Type d'objet	Source
Maersk	4 000	Serveurs	Wired [28], Zdnet [32]
Maersk	45 000	Ordinateurs réinstallés	Wired [28], Zdnet [32]
Maersk	2 500	applications	Zdnet [32]
Mondelez	1 700	Serveurs	New York Times [33]
Mondelez	24 000	Ordinateurs	New York Times [33]

Tableau 34 - Dégâts informatiques de NotPetya

Le tableau précédent présente les dégâts causés par NotPetya sur Maersk et Mondelez. Nos utiliserons ces informations au moment de construire notre fonction de coût permettant de passer d'une entreprise infectée par le virus à un coût économique.

Nous avons aussi appris qu'une des grandes erreurs des hackers de WannaCry a été de laisser la possibilité d'activer un kill-switch en rachetant simplement un nom de domaine libre. Cette erreur a permis de stopper l'attaque relativement rapidement. Pour NotPetya, les hackers n'ont pas commis une telle erreur mais des experts ont rapidement découvert qu'on pouvait immuniser son système en empêchant le virus de s'exécuter grâce à la création d'un simple fichier [34]. La progression de l'attaque a donc été stoppée en quelques heures. Pour l'estimation des paramètres du modèle, nous pourrons donc utiliser un horizon de temps fixé à 24 heures [35] tandis que pour les simulations, le temps nécessaire pour endiguer le virus sera donné par la variable aléatoire T_P.

3.2.5 Construction du modèle ransomware

Détaillons l'application du scénario ransomware. L'objectif est ici d'introduire la structure du modèle tout en explicitant au fur et à mesure les variables utilisées par le modèle. Les hypothèses sous-jacente à notre modélisation seront énoncées et justifiées. Le rôle de chacun des modules sera détaillé et nous montrerons comment a été construite la fonction de coût économique h. Les paramètres du modèle seront estimés dans la partie 3.

Nous émettons les hypothèses suivantes pour construire le modèle ransomware.

Hypothèse i) : La population est supposée fermée et constante.
Justification : Le portefeuille AXA est suffisamment grand et diversifié pour représenter une portion de l'économie mondiale. Nous supposerons donc que les effets observés sur notre portefeuille s'appliquent à la population mondiale. Ainsi, supposer la population fermée et constante est raisonnable puisque notre portefeuille d'assurés est stable sur une année.

Hypothèses ii) : le taux de transmission α est considéré comme propre au virus et sera donc le même pour tous les assurés. Il est amené à varier d'une attaque à l'autre. Au contraire, les temps de réparation et infectieux sont propres aux assurés. Par rapport au modèle SIR déterministe classique présenté en 3.1.2.3), nous retirons donc le paramètre β et tirons aléatoirement des temps infectieux pour chaque entreprise.
Justification : Nous estimons que la capacité d'un virus à infecter d'autres victimes est lié à la faille de sécurité exploitée et dépend donc principalement du code écrit par les hackers. Ce taux n'est donc pas amené à évoluer au cours d'une attaque. En revanche, une fois une entreprise infectée, ses caractéristiques et pratiques informatiques influencent la durée infectieuse et de réparation. Des temps infectieux propres à chaque victime sont donc tirés et pourront plus tard différer selon le profil informatique des assurés. Contrairement au modèle déterministe où à chaque pas de temps une proportion β d'entreprises migrait du compartiment I au compartiment R, cette proportion n'est ici pas constante puisque les temps infectieux stochastiques régissent le passage de I à R. On autorise donc une certaine volatilité autour de la proportion d'entreprises qui migrent de I à R d'un pas de temps à l'autre, ce qui influe sur la diffusion du virus et permet de générer des scénarios différents.
Hypothèse iii) : on considère que le ransomware exploite une faille de sécurité présente sur un système d'exploitation. La population susceptible est tirée aléatoirement selon les parts de marché des systèmes d'exploitation.

Justification : les deux ransomwares les plus dévastateurs, NotPetya et WannaCry utilisaient tous deux une faille de sécurité présente sur Windows. Nous n'avons pas encore d'information sur les profils informatiques de nos assurés ; au lieu de sélectionner les assurés utilisant le système attaqué, nous tirons pour le moment les assurés vulnérables au ransomware de manière aléatoire selon les parts de marché des systèmes d'exploitation.

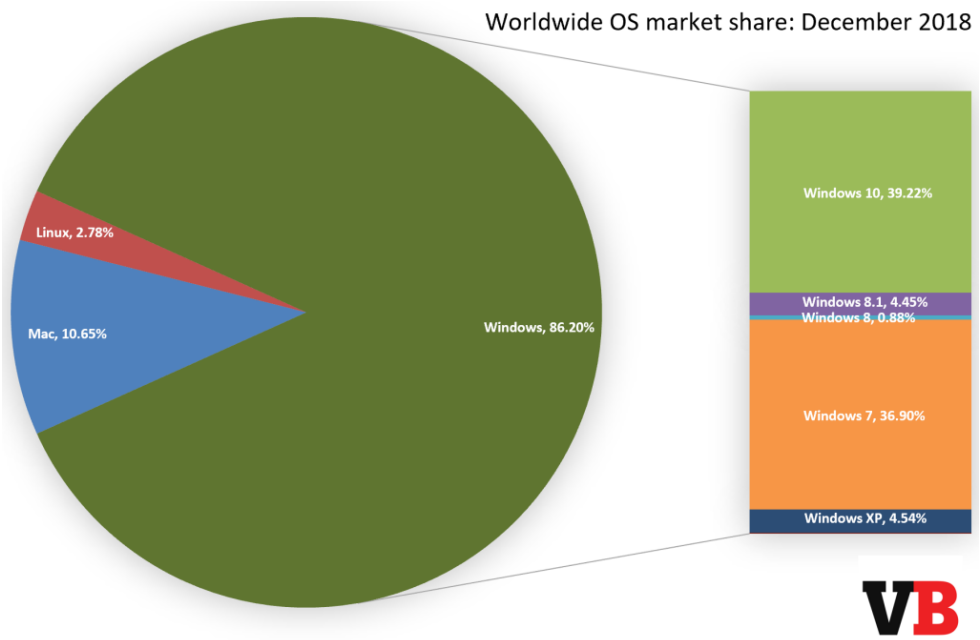


Figure 20- Part de marché des systèmes d'exploitation- Source Venturebeat.com [**36**]

Hypothèse iv) : Pour sélectionner la population initialement vulnérable, on prend une probabilité uniforme sur les différents systèmes d'exploitation attaqués et on considère que si un système Windows est vulnérable, tous les systèmes Windows antérieurs le sont aussi.
Justification : Il serait préférable de tirer directement les entreprises de notre portefeuille correspondant à un système informatique précis, mais nous n'avons pas ce degré de précision sur nos assurés. Nous tirons donc selon les parts de marché, ce qui est acceptable au vu de la diversification de notre portefeuille. Microsoft arrête peu à peu de développer des mises à jour sur les versions de Windows antérieures à Windows 10 [37]. Il est donc raisonnable de penser que plus la version est ancienne, plus il est probable qu'elle comporte une faille de sécurité. Nous n'écartons pas les autres systèmes d'exploitation d'une potentielle attaque ransomware.
On obtient le tableau suivant à partir de la figure 24 et de l'hypothèse iv) :

Système d'exploitation	Part de marché	Pourcentage de susceptibles si attaqué	Probabilité d'attaque
Linux	0,0278	0,0278	1/6
Mac	0,1065	0,1065	1/6
Windows 10	0,3922	0,8599	1/6
Windows 8	0,0533	0,4677	1/6
Windows 7	0,369	0,4144	1/6
Windows XP	0,0454	0,0454	1/6
Unknown	0,0058	0,0058	0

Tableau 35-Probabilité des proportions de susceptibles

A partir de ces hypothèse, nous avons construit le modèle ransomware qui fonctionne de la manière suivante :

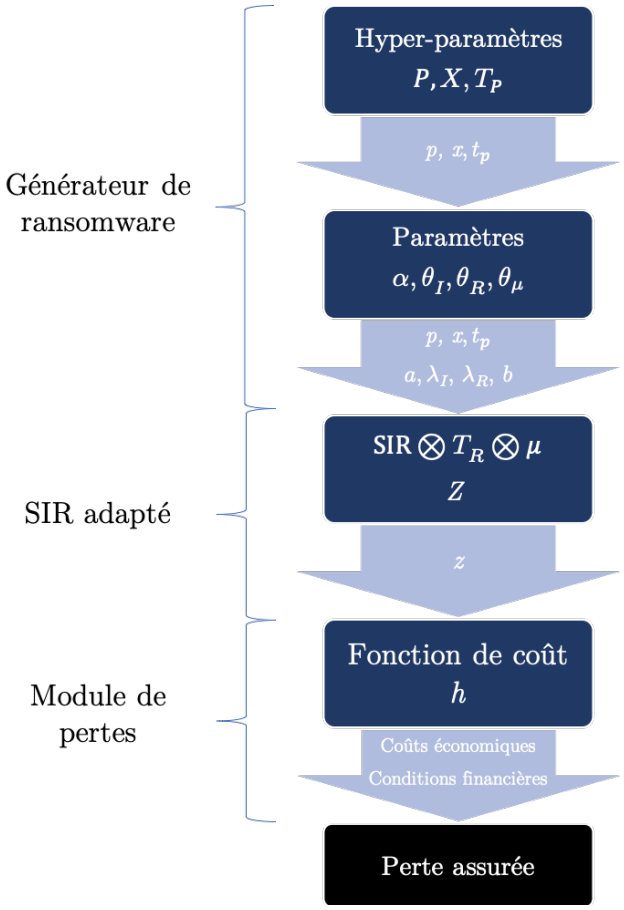


Figure 21 – Fonctionnement du Modèle ransomware

Détaillons le rôle de chacun des modules et variables afin d'expliquer le schéma précédent.

3.2.5.1 Le générateur de ransomware

Il produit les paramètres et hyper-paramètres propres à chaque attaque ransomware. Ces hyper-paramètres et paramètres modélisent les caractéristiques de l'attaque et suivent chacun une loi de probabilité que nous allons spécifier dès à présent.

Nous avons comme hyper-paramètres :
- P, la variable aléatoire qui donne la proportion d'individus vulnérables au virus. P suit une loi uniforme sur l'ensemble $\{0.0278, 0.1065, 0.8599, 0.4677, 0.4144, 0.0454\}$ obtenu grâce au tableau 35
- X, la variable aléatoire à valeurs dans $\mathbb{R}_+^*$ qui détermine le coût de la rançon en dollars.
- T_P, la variable aléatoire à valeurs dans $\mathbb{R}_+^*$ qui modélise le temps avant qu'un patch soit développé et que l'attaque soit endiguée. On note θ_P le vecteur de paramètres de sa loi.

Notons p, x et t_P les réalisations respectives de P, X et T_P.
Conditionnellement à ces réalisations, on a les paramètres suivants :
- α, la variable aléatoire à support dans [0,1] modélisant le taux de transmission du virus
- θ_I, la variable aléatoire à support dans $\mathbb{R}_+^*$ donnant le paramètre d'intensité de la loi exponentielle des temps infectieux.

- θ_R, la variable aléatoire à support dans $\mathbb{R}_+^*$ donnant le paramètre d'intensité de la loi exponentielle des temps de réparation.
- θ_μ, la variable aléatoire donnant la borne supérieure de la sévérité des dégâts. Cette sévérité s'exprime en pourcentage d'ordinateurs infectés et a donc comme support]0,1[. $\theta_\mu$vit donc dans]0,1[(en étant supérieur à la borne inférieure de la sévérité).

Nous obtenons la réalisation $(a, \lambda_I, \lambda_R, b)$ de $(\alpha, \theta_I, \theta_R, \theta_\mu | P = p, X = x, T_P = t_P)$.
A partir de toutes ces informations, notre SIR adapté est en mesure de simuler une attaque ransomware.

3.2.5.2 Fonctionnement du SIR adapté

Étant donnés p, x, t_P, a, λ_I, λ_R et b transmis par le générateur, notre SIR adapté simule une processus stochastique qui nous fournit des observations. Notre SIR adapté est une version particulaire du modèle SIR déterministe à laquelle on a ajouté un temps de réparation et des sévérités individuelles au compartiment R. Chaque assuré représente une particule et la population n'est plus vue comme un tout. Cette vision particulaire nous permet de simuler au niveau de chaque police des temps infectieux, de réparations et la sévérité des dégâts qui auront une influence sur le coût assuré associé à la police. Justifions le choix des lois paramétriques avant de détailler le fonctionnement du SIR adapté.

Choix de lois paramétriques pour les temps infectieux, temps de réparation et la sévérité des dégâts
Pour les temps infectieux et les temps de réparation on décide de se donner des lois de durée simples. Nous choisissons des lois exponentielles car ce sont des lois de durée classiques faciles à manipuler et nous observons que la variance de l'échantillon du tableau 33 *« Temps des réparations totales et de reprise de l'activité »* est proche (mais légèrement inférieure) du carré de sa moyenne. On rappelle que pour une variable T suivant une loi exponentielle de paramètre λ, $\mathbb{E}(T) = \frac{1}{\lambda}$ et $\mathbb{V}(T) = \frac{1}{\lambda^2}$. De plus, n'ayant pas d'informations permettant de soutenir une hypothèse de fonction de hasard croissante ou décroissante pour nos lois de durée, nous faisons le choix central de prendre une loi exponentielle dotée d'une fonction de hasard constante égale à λ.
En notant T_I la variable aléatoire régissant les temps infectieux d'une attaque on a $T_I \sim \varepsilon xp(\lambda_I)$
En notant T_R la variable aléatoire régissant les temps de réparation d'une attaque on a $T_R \sim \varepsilon xp(\lambda_R)$
Pour chaque police touchée on tire selon μ le pourcentage d'ordinateurs impactés.
Nous prenons $\mu \sim U(0.1, b)$. Pour la sévérité μ on se donne une variable aléatoire uniforme entre 0.1 et $b < 1$. Nous excluons 0 car cela correspond à un assuré non touché et nous excluons 1 car si l'intégralité des systèmes sont corrompus alors l'entreprise est en quelque sorte définitivement hors service. Nous n'envisageons pas ce cas et supposons que les entreprises parviennent à isoler une part de leurs systèmes informatiques qui leur permettra de reprendre leur activité.

Notations : $K(t)$ est le nombre d'individus dans K à l'instant t.
$\varepsilon(K, t)$ est l'ensemble des individus dans K à l'instant t.

Expliquons maintenant comment notre SIR adapté simule des entreprises infectées avec leurs temps infectieux, leurs temps de réparation et leurs sévérités des dégâts.

Le générateur transmet au SIR les valeurs de p, x, t_P, a, λ_I, λ_R et b pour procéder à la simulation. Le SIR adapté utilise tous ces paramètres sauf x, le coût de la rançon, qui sera utilisé au sein du module de pertes.
t_P fixe la durée maximum de propagation du ransomware tandis que a régit la propagation du virus du temps 0 jusqu'au temps t_P.

Compartiment S
Au temps 0 on tire la population susceptible initiale $\varepsilon(S, 0)$ qui correspond à une proportion p de notre portefeuille, tirée uniformément avec stratification sur la variable catégorielle de taille d'entreprise. Une première entreprise est infectée au temps 0. On simule son temps infectieux selon la loi de T_I. A chaque pas de temps t jusqu'à t_P :
on tire uniformément avec stratification sur la variable catégorielle de taille d'entreprise $a\frac{I(t)}{N}S(t)$ nouveaux infectés qui vont dans le compartiment I (en arrondissant à l'entier supérieur, ce qui permet d'avoir automatiquement 2 infectés au temps 1 et ainsi pouvoir modéliser un évènement d'accumulation). Ces tirages supposent implicitement l'hypothèse suivante :
Hypothèse v) :
Nous considérons que notre population est homogène et totalement mélangée et que chaque infecté peut contaminer n'importe quel susceptible avec un même taux de transmission du virus.
De plus pour toute attaque, si une catégorie de taille d'entreprises représente une certaine proportion de l'économie, elle représentera cette même proportion au sein des infectés.
Justification :
Le risque cyber étant systémique et imprévisible, cette hypothèse est acceptable. Nous supposons des liens entre les assurés mais leur nature n'est pas modélisée. Ainsi, nous ne supposons pas qu'un type de lien particulier favorise la propagation du ransomware, ce qui revient à prendre en compte le caractère évolutif du risque. Un échange direct de mail ou une collaboration ne sera pas nécessairement le prochain vecteur de propagation d'un nouveau virus informatique.
NotPetya a touché toutes tailles d'entreprises. Afin de reproduire un phénomène semblable, nous tirons les entreprises infectées en utilisant un tirage uniforme avec stratification sur la variable catégorielle de taille d'entreprise. Notre portefeuille étant très grand, cela nous évite d'avoir des tirages d'infectés concentrés uniquement sur une catégorie de taille d'entreprises. De plus, le portefeuille AXA est suffisamment grand et diversifié pour refléter une fraction de l'économie mondiale.

Compartiment I
À chaque contaminé arrivant dans le compartiment I on associe un temps infectieux t_I tiré selon la loi de T_I. Pour une même attaque, les temps infectieux sont indépendants et identiquement distribués selon la loi de T_I.
Chaque individu reste dans le compartiment I pendant son propre temps infectieux, durant lequel il infecte potentiellement des susceptibles. Une fois cette durée atteinte, l'individu a coupé ses systèmes infectés de tout réseau et va donc dans le compartiment retiré. Lorsque t_P la durée maximum de l'attaque atteinte, tous les individus infectés encore présents dans I vont dans le compartiment R.

Compartiment R
C'est ici que s'effectue notre principale modification par rapport à un SIR classique : une fois arrivées dans le compartiment R, il est temps pour les victimes du ransomware d'évaluer leurs dégâts. Pour chaque victime, on tire une sévérité u selon la loi de μ et un temps de réparation t_R avant la reprise d'une activité normale selon la loi de T_R. Les sévérités et les temps de réparation d'une même attaque sont indépendants et identiquement distribués selon respectivement la loi de μ et la loi de T_R. On

remarque donc une sévérité commune au sein d'une attaque. Les pertes assurées issues d'un même évènement ne seront pas indépendantes.

Pour simuler notre SIR adapté, nous procédons de manière itérative avec un schéma d'Euler.
Notre modèle permet donc de générer des réalisations d'une variable aléatoire Z dont nous allons détailler la structure.
Une réalisation statistique z_k de Z contient les victimes, les temps infectieux, les temps de réparation et les sévérités. Pour un virus ayant fait m victimes au total on écrit :

$$z_k = \left(\begin{bmatrix} victime_{k,1} \\ \vdots \\ victime_{k,i} \\ \vdots \\ victime_{k,m} \end{bmatrix}, \begin{bmatrix} t_{I\,k,1} \\ \vdots \\ t_{I\,k,i} \\ \vdots \\ t_{I\,k,m} \end{bmatrix}, \begin{bmatrix} t_{R\,k,1} \\ \vdots \\ t_{R\,k,i} \\ \vdots \\ t_{R\,k,m} \end{bmatrix}, \begin{bmatrix} u_{k,1} \\ \vdots \\ u_{k,i} \\ \vdots \\ u_{k,m} \end{bmatrix} \right)$$

Pour alléger la notation, nous avons noté uniquement le vecteur de victimes, mais ce dernier contient en réalité toutes les informations connues dans les victimes du portefeuille AXA.
La loi de la variable aléatoire Z dépend des lois de l'ensemble des paramètres et hyper-paramètres du modèle. On note D_Z l'espace d'état de Z, qui dépend de notre portefeuille d'assurés. Si le modèle génère m victimes pour la simulation z_k, alors z_k est de dimension $4m$. On remarque ici que la dimension des réalisations de Z n'est pas fixe : Z garde une structure stable de quatre composantes mais ces dernières sont de taille variable puisqu'elles dépendent du nombre de victimes générées par l'attaque. Nous noterons $z_{k,i}$ la réalisation z_k du modèle pour laquelle les composantes sont restreintes à la victime i.

3.2.5.3 Module de pertes et construction de la fonction de coût h

Une fois Z simulée par le SIR adapté, on applique une fonction de coût économique h qui prend en entrée le type de malware, le temps infectieux et de réparation, les caractéristiques des victimes et renvoie un coût économique par type de sous-garantie.

Le module de perte fonctionne en deux étapes. La première étape permet d'associer à une réalisation z un coût économique par victime réparti sur certaines sous-garanties. Cette opération est réalisée par la fonction de coût économique notée h que nous allons construire dès à présent. La seconde étape consiste à appliquer les conditions financières des contrats afin d'obtenir la perte assurée par victime. En sommant les pertes assurées de chaque victime on obtient la perte totale supportée par l'assureur.

Construisons la fonction de coût h en utilisant les informations à notre disposition sur NotPetya. Grâce aux informations présentées sur NotPetya, on sait que notre fonction de coût doit être capable de générer des pertes allant de centaines de millions d'euros à quelques dizaines de milliers d'euros.
Le paramètre de sévérité modélisé par μ va nous aider à introduire cette grande amplitude.
Cette fonction donnera la perte par sous-garantie affectée à une entreprise contaminée par un ransomware. Pour cela, nous avons d'abord besoin de variables intermédiaires.

Nous voulons utiliser la taille de l'entreprise comme une variable croissante du coût. Justifions cette hypothèse. A l'aide de la base BLI complétée nous sommes en mesure d'affecter une taille aux entreprises. Nous voulons vérifier si les classes 'Small' et 'Large' de taille d'entreprise (selon une convention propre à AXA) ont des coûts associés différents lors d'attaques cyber. Pour ce faire, Nous effectuons un test de Mann-Whitney pour savoir si la loi du nombre de données perdues est la même

pour les petites et les grandes entreprises. Rappelons que le test de Mann Whitney est un test non paramétrique basé sur les rangs des deux échantillons mis en commun. L'hypothèse nulle H0 est « les deux échantillons suivent la même loi » tandis que l'hypothèse alternative H1 est « l'échantillon des grandes entreprises a tendance à prendre des valeurs plus grandes que l'échantillon des petites entreprises ». Nous obtenons une p-value de 0.028, ce qui nous permet de rejeter H0 à un seuil de confiance de 5%. Le nombre de données perdues est donc plus petit pour les entreprises de petite taille que pour les entreprises de grande taille. Dès 2014, Jay Jacobs [38] a montré que le coût d'un *data breach* était une fonction croissante du nombre de données perdues. Cette relation de corrélation positive entre ces deux variables peut facilement être retrouvée à partir de la base Veris 2019.
Nous pourrons donc utiliser le chiffre d'affaires et le nombre d'employés (proportionnels à la taille d'une entreprise) pour déterminer la perte économique.

On décide de modéliser la perte économique d'une entreprise, c'est-à-dire brute d'assurance, comme étant répartie en 4 catégories correspondant à des sous-garanties cyber *affirmative First Party*. Ces 4 catégories sont :
- CYL (Data and Software Loss)
- CRE (Cyber Ransom Extorsion)
- IRC (Incident Response Cost)
- BI (Business Interruption)

Avant de détailler les expressions donnant la perte économique par sous-garantie, nous allons d'abord introduire les variables utilisées par notre fonction.
Rappelons que les seules variables à notre disposition sont pour l'instant le secteur d'activité, le chiffre d'affaires et le pays de l'assuré. Les proxies que nous allons présenter ici pourront être remplacés par leurs valeurs exactes lorsque les données collectées sur les assurés le permettront.

- **Nombre d'ordinateurs**

Nous utilisons la base 2018 de l'Organisation du Coopération et de Développement Économique (OCDE) sur les Technologies de l'Information et des Communications (TIC) dans les entreprises. Cette base est disponible en ligne [39] et présente notamment le pourcentage d'employés utilisant un ordinateur selon le secteur et selon le pays (tableau à double entrée). Ces informations sont renseignées à une fréquence annuelle et comportent de nombreuses données manquantes. Les points manquants présentant une structure particulière (absence totale d'informations pour certains pays), nous ne pouvons pas utiliser de GLM en prenant le pays et le secteur comme variables pour estimer les pourcentages manquants.
Nous n'avons besoin que de deux années : 2017 (année de NotPetya) et 2019 (année de nos simulations). 2019 n'étant pas encore disponible, on utilisera 2018.
Pour chaque secteur, on procède de la manière suivante pour compléter les valeurs manquantes :
- si pour un pays la valeur est manquante mais présente pour des années de N-1, N-2, N+1 alors on prend la valeur la plus proche en favorisant la plus récente.
- si la valeur n'est pas non plus présente pour les années voisines, alors on prend la moyenne des pays dont le développement économique est jugé 'semblable'. Par exemple, pour les États-Unis dont quasi toutes les valeurs sont manquantes, on prendra pour chaque secteur la moyenne des valeurs renseignées pour la France, l'Allemagne et le Royaume-Uni.

Nous avons maintenant à notre disposition une base donnant le pourcentage d'employés utilisant un ordinateur par secteur selon les pays. Nous avons donc besoin du nombre d'employés afin de pouvoir estimer un nombre d'ordinateurs pour chaque assuré. Une table de correspondance interne à AXA permet d'estimer le chiffre d'affaires par employés de l'assuré en fonction de son pays et de son secteur d'activité. Une fois le nombre d'employés calculé grâce à cette table, nous sommes en mesure d'affecter un nombre d'ordinateur à chaque assuré.
En notant o_i l'estimation du nombre d'ordinateurs de l'assuré i on a :

$$o_i = e_i \times p_i$$

avec :
e_i l'estimation du nombre d'employés de l'assuré i
$p_i$le pourcentage d'employés utilisant un ordinateur dans le pays et pour le secteur de l'entreprise i .
Au sein d'une entreprise, le nombre d'ordinateurs touchés par une attaque ransomware sera $o_i \times u_i$.

- **Nombre de serveurs**

Le nombre de serveurs est obtenu à partir du nombre d'ordinateurs. On suppose 20 ordinateurs par serveur [40] . En notant s_i le proxy du nombre de serveurs de l'entreprise i on a :

$$s_i = \frac{o_i}{n_s}$$

avec :
n_s =20, le nombre d'ordinateurs par serveur,

L'étude à partir de laquelle a été trouvé ce chiffre n'étant pas très récente, nous avons pris la valeur moyenne de la variable sans distinction de secteur. L'effet secteur est déjà pris en compte grâce à la table de l'OCDE qui est bien plus récente. Pour vérifier si l'ordre de grandeur est cohérent, on regarde nos données trouvées sur Maersk et Mondelez : le nombre d'ordinateurs touchés divisé par nombre de serveurs réinstallés donne respectivement 11,25 et 14, ce qui est du même ordre de grandeur que notre ratio de 20 commun à tous les secteurs.

- **Chiffre d'affaires journalier**

Il est simplement obtenu en divisant par 365 le chiffre d'affaires total de l'assuré.
On le note d_i (pour 'daily turnover') le chiffre d'affaires journalier de l'assuré i.

- **Le coût de la rançon**

Le coût de la rançon est donné par le générateur de virus, Il est modélisé par une variable aléatoire notée X. Il correspond au montant exigé par les hackers pour déverrouiller un ordinateur contaminé.

- **Pourcentage d'ordinateurs qui payent la rançon.**

On note *paid* ce pourcentage. Les rançons étant peu souvent payées, on fixe ce taux à 5% : nous pensons que le pourcentage d'ordinateurs payant la rançon restera faible puisque ni les experts en cyber sécurité ni les assureurs ne recommandent de payer les rançons. En effet, il est impossible de s'assurer que le déblocage des systèmes et le déchiffrement des données sera bien effectué après paiement de la rançon. De plus, le paiement de cette rançon pause aussi des problèmes éthiques : payer le hacker encourage l'apparition d'autres attaques.

- **Le temps avant la reprise d'activité**

On note t_i la durée en jours avant la reprise d'une activité normale de l'entreprise i. Cette durée est la somme de $t_{I,i}$ converti en jours et de $t_{R,i}$. Autrement dit : $t_i = \frac{t_{I,i}}{24} + t_{R,i}$.

- **La sévérité avec laquelle est touché l'assuré**

Cette sévérité notée u_i représente la part des systèmes de l'assuré i qui sont touchés. Elle est donc comprise entre 0 et 1.

Nous avons maintenant les variables nécessaires pour construire la fonction de coût.
Lorsqu'une entreprise du portefeuille prise touchée, elle est renseignées dans le vecteur Z_k avec toutes ses caractéristiques (pays, chiffre d'affaires journalier, nombre d'employés, secteur d'activité, nombre d'ordinateurs, nombre de serveurs) ainsi que ses temps infectieux et la durée avant la reprise normale de l'activité simulés par le modèle. Tous ces éléments, auxquels s'ajoutent le coût de la rançon et le pourcentage de paiements vont nous permettre de calculer C_i, la perte économique subie par l'assuré i.
Cette perte est construite à partir de 4 termes :

$$h\colon D_Z \mapsto \mathbb{R}$$
$$C_i = h(z_{k,i}) = C_{i,CYL} + C_{i,CRE} + C_{i,IRC} + C_{i,BI}$$

Détaillons la construction de chacun de ces termes.
Nous prendrons l'exemple de Maersk et de Mondelez pour vérifier la pertinence de nos formules. Notons que dans notre modélisation, Maersk aurait eu une sévérité u_i égale à 0.56. En effet, Maersk - transporteur danois- possède un pourcentage d'employés utilisant un ordinateur qui s'élève à 100%. Maersk emploie 80 220 personnes et a donc un parc de $80\,220 \times 100\% = 80\,220$ ordinateurs. On obtient la valeur de la réalisation de μ en prenant nos 45 000 ordinateurs touchés du tableau 34 divisés par le nombre total d'ordinateurs, ce qui donne une sévérité $u_i = 0.56$. Pour Mondelez le modèle donnerait une sévérité de 0.38. En effet, Mondelez est une multinationale agroalimentaire américaine qui emploie 107 000 personnes dans le monde. La table OCDE donne un pourcentage de 59.23% des employés qui utilisent un ordinateur. On a donc un total de 63 376 ordinateurs dont 24 000 impactés toujours d'après le tableau 34 ce qui donne un ratio de 0.38.

- **CYL (Data and Software Loss)**

Cette sous-garantie rassemble la perte ou dégradation de données et de logiciels survenue à la suite du ransomware. Nous supposons que les données des entreprises sont réparties sur des serveurs de 1TB[1]. Avec notre hypothèse de 20 ordinateurs par serveur on obtient en moyenne 50GB par utilisateur. Nous supposons que les données de chaque serveur coûtent 1300USD$ à décrypter [41].
$C_{i,CYL} = u_i \times s_i \times 1\,300$
Pour Maersk on obtient $4\,000 \times 1\,300 = 5.2$ millions de dollars.
Pour Mondelez on obtient $1\,700 \times 1\,300 = 2.2$ millions de dollars

- **CRE (Cyber Ransom Extorsion)**

Cette sous-garantie correspond à la perte due au paiement de la rançon. Seul un pourcentage *paid* d'ordinateurs touchés $u_i \times o_i$ paye la rançon dont le coût s'élève à x dollars. On a donc :

[1] TB signifie Tera Byte soit 1 000 Giga Bytes (GB).

$C_{i,CRE} = u_i \times o_i \times x \times paid$
Pour Maersk on obtient $45\ 000 \times 600 \times 5\% = 1.35$ millions de dollars.
Pour Mondelez on obtient $24\ 000 \times 600 \times 5\% = 0.72$ millions de dollars

- **IRC (Incident Response Cost)**

Cette sous-garantie correspond au remboursement des coûts directement liés à un incident cyber, comme par exemple les frais d'investigation puis de nettoyage des systèmes informatiques ou encore la réinstallation de programmes endommagés. On prend ici le pire coût possible en modélisant le coût de remplacement des ordinateurs touchés. On compte 400 dollars par ordinateur. [42]
$C_{i,IRC} = u_i \times o_i \times 400$
Pour Maersk on obtient $45\ 000 \times 400 = 18$ millions de dollars.
Pour Mondelez on obtient $24\ 000 \times 400 = 9.6$ millions de dollars

- **BI (Business Interruption)**

Ce terme correspond à la perte d'activité survenue suite à l'attaque cyber. Cette garantie couvre la perte de bénéfices survenue suite à un évènement cyber.

Dans un premier temps nous avons proposé la formule suivante :
$C_{i,BI} = u_i \times t_i \times taux\ de\ marge \times d_i$
Avec $d_i \times taux\ de\ marge$ qui représente donc le bénéfice journalier de l'entreprise. Cette formule suppose que la production de $b\%$ de bénéfices nécessite l'utilisation de $b\%$ des ordinateurs de l'entreprise. On a $u_i\%$ d'ordinateurs touchés donc quotidiennement $u_i \times d_i \times taux\ de\ marge$ euros perdus et cela pendant une durée t_i.

Les données recensées présentent la perte de chiffre d'affaires et non de bénéfices, nous fixons donc le facteur multiplicatif *taux de marge* à 1 pour calibrer la fonction de coût sur le chiffre d'affaires perdu et ferons de même pour l'estimation des paramètres du modèle.

On cherche à vérifier si cette relation est cohérente pour Maersk. Son chiffre d'affaire quotidien s'élève à 106.44 millions de dollars. On sait que Maersk a nécessité 10 jours avant de reprendre une activité normale. La perte BI calculée via cette méthode s'élève donc à $0.56 \times 106.44 \times 1 \times 10 = 597.12$ millions de dollars. On a donc deux fois la perte totale de Maersk sur une seule garantie : cette méthode n'est pas satisfaisante.

Pour revoir à la baisse cette estimation, on émet l'hypothèse supplémentaire qu'un assuré répare chaque jour une même proportion de ses dommages jusqu'à pouvoir reprendre une activité normale. Ces dommages peu à peu réparés, l'assuré reprend progressivement son activité.
Nous remplaçons donc le terme t_i par la $\sum_{k=0}^{t_i-1} \frac{t_i-k}{t_i}$. Chaque jour, l'assuré répare $\frac{1}{t_i}$. Le premier jour il perd donc l'intégralité des $u_i \times d_i$ dollars de chiffre d'affaire. Le second jour il perd $\frac{t_i-1}{t_i} \times u_i \times d_i$ dollars de chiffre d'affaires. Le k$^{\text{ième}}$ jour il perd $\frac{t_i-k}{t_i} \times u_i \times d_i$ dollars de bénéfices et ainsi de suite. On a $\sum_{k=0}^{t_i-1} \frac{t_i-k}{t_i} = \sum_{k=1}^{t_i} \frac{k}{t_i} = \frac{1}{t_i}\frac{(t_i+1)t_i}{2} = \frac{(t_i+1)}{2}$
On obtient donc : $C_{i,BI} = u_i \times d_i \times taux\ de\ marge \times \frac{(t_i+1)}{2}$

Ce qui nous donne pour Maersk une perte de $0.56 \times 106.44 \times 1 \times \frac{10+1}{2} = 327.8$ millions de dollars pour la garantie BI.
Pour Mondelez on obtient $0.38 \times 81.09 \times 1 \times \frac{15+1}{2} = 245.7$. (Nous avons pris comme durée de réparation avant la reprise d'une activité normale la durée totale de réparation du tableau 33 multiplié par le coefficient de proportionnalité $\frac{10}{23}$).

Nous conservons cette approche puisqu'en sommant toutes les sous-garanties on obtient pour Maersk 352.35 millions de dollars, ce qui est assez proche des 300 millions de perte totale réellement comptabilisés après NotPetya tandis que pour Mondelez on obtient 258.22 millions contre 188 millions réellement comptabilisés.

Conclusion : Nous avons présenté le modèle ransomware permettant de simuler le déroulement d'une attaque cyber reposant sur un ransomware. Ce modèle statistique permet de générer des victimes munies de leurs temps infectieux et de leurs temps de réparation, ainsi qu'une sévérité modélisant la part des systèmes informatiques touchés. La fonction de coût économique h construite à partir d'informations relatives à NotPetya permet de passer d'une simulation z générée par le modèle ransomware à un coût économique individuel réparti en garanties. La perte totale de l'évènement est obtenue en sommant les coûts individuels. Une question naturelle apparaît : quelle valeur ou loi donner aux paramètres du modèle pour simuler des z réalistes ? Nous proposons une réponse à cette question dans la partie suivante.

3.3 Estimation des paramètres

Dans cette partie, nous détaillons la méthode d'estimation des paramètres du scénario ransomware.
Nous introduisons et justifions d'abord le choix du cadre bayésien avant d'aborder la méthode ABC et expliquer son choix d'utilisation par rapport à MCMC.
Étant dans un cadre bayésien, l'objectif de l'estimation sera de trouver la loi *a posteriori* des paramètres du modèle permettant de reproduire des évènements proches de NotPetya.

Pour ce faire, les hyper-paramètres seront fixés à leurs valeurs connues pour NotPetya :
- X, le coût de la rançon sera fixé à 600 dollars
- T_P, le temps avant le patch sera fixé à 24 heures
- P, la proportion de vulnérables sera fixée à 46.77%, cette valeur correspond aux systèmes Windows antérieurs à Windows 10[1]. Ces trois hyper-paramètres fixés pour l'estimation de la loi *a posteriori* seront ensuite rendus aléatoires pour la simulation de la perte assurée, ce qui nous permettra de nous affranchir des conditions spécifiques de NotPetya pour simuler d'autres évènements vraisemblables.

Dans le cadre de cette étude on s'intéresse donc à estimer la loi *a posteriori* des paramètres α, θ_I, θ_R et θ_μ.

[1] Pour NotPetya tous les systèmes utilisant Windows excepté ceux dotés de Windows 10 dernièrement mis à jour étaient vulnérables au virus.

Nous émettons l'hypothèse suivante :
Hypothèse vi) : Notre portefeuille supporte 10% de NotPetya, tant en coût total qu'en nombre de victimes. On veut donc estimer notre modèle statistique tel que notre portefeuille ait environ 200 victimes subissant une perte de 1 milliard USD$.
Justification : On considère que les entreprises du portefeuille AXA sont ni plus ni moins risquées que les autres entreprises dans le monde et représentent 10% de l'économie mondiale. Cette hypothèse est conservatrice puisqu'AXA détient en réalité 10% du marché de l'assurance cyber. Or, ce marché ne représente pas la totalité de l'économie mondiale.

Notre portefeuille a connu une croissance de 15% entre 2017 et 2019. N'ayant pas accès au portefeuille de 2017, nous divisons la proportion de vulnérables par 1.15 pour estimer les paramètres du modèle sur un portefeuille réduit. L'idéal serait d'estimer le modèle avec toutes les données de 2017, puis de simuler sur les données 2019, mais nous n'avons pas à disposition ces bases de données.
Précisons dès à présent que dans cette troisième partie concernant l'estimation, tous les coûts retournés par les modèles sont des coûts économiques en euros[1].

3.3.1 Choix du cadre bayésien

Le cadre bayésien apparait naturellement pour mettre à profit les connaissances que nous avons acquises sur NotPetya et les ransomware de manière générale. En effet, le cadre bayésien permet de munir l'espace des paramètres du modèle de lois *a priori* afin d'introduire une expertise sur le problème considéré. L'information tirée des observations couplée à des connaissances acquises *a priori* permettent d'estimer la loi a posteriori. L'estimation de la loi *a posteriori* nous permettra d'ajouter une notion d'incertitude sur les paramètres du modèle. On veut apprendre d'une attaque pour regarder ce qu'il peut potentiellement se passer dans le futur.

On note $f(z|\theta)$ la vraisemblance (ou *likelihood*) du modèle ransomware.
Dans le cadre bayésien, on introduit une incertitude sur le paramètre d'intérêt θ donnée par une loi de probabilité, nommée loi *a priori* (*prior*) et notée $\pi(\theta)$. La loi a posteriori est une mise à jour de la loi a priori conditionnellement aux observations et est donnée par la formule de Bayes *:*

$$\pi(\theta|z) = \frac{f(z|\theta)\pi(\theta)}{m(z)}$$

$$\propto f(z\ |\theta)\pi(\theta)$$

avec :
$m(Z) = \int_{\theta\in\mathbb{R}^4} f(\ z|\ \theta)\pi(\theta)d\theta$ la densité marginale de Z aussi appelée *evidence.*

Nos travaux consisteront à estimer :
- la loi du taux de transmission α, à support dans [0,1]
- la loi de θ_I, à support dans $\mathbb{R}_+^*$
- la loi de θ_R, à support dans $\mathbb{R}_+^*$
- la loi des bornes du support du μ, c'est-à-dire θ_μ qui est donc de dimension 2 et à support dans [0,1] ×[0,1] avec la première composante strictement inférieure à la seconde.

Autrement dit, le paramètre d'intérêt de notre étude est $\theta = (\alpha, \theta_I, \theta_R, \theta_\mu)$.

[1] Les variables en dollars utilisées par le modèle sont converties en euros en utilisant le taux USD/EUR= 0.874. Les données de portefeuille ont toutes été converties en euros.

Si nous notons y la réalisation correspondant à NotPetya suivant notre modèle, remarquons que nous n'avons pas accès à l'ensemble des variables. Les deux informations principales que nous avons sur l'évènement sont le nombre de victimes et le coût total. Nous ne connaissons pas explicitement la vraisemblance du modèle $f(z|\theta)$, qui est difficilement calculable puisqu'elle dépend des profils de chaque assuré dans le portefeuille. Nous n'avons pas non plus accès à l'observation complète de Z correspondant à NotPetya ni à une quelconque observation historique de Z pour un virus informatique.

De ce fait, il est impossible de recourir à la méthode MCMC qui est la plus répandue pour estimer les paramètres d'un modèle épidémiologique. En effet, la méthode MCMC consiste à générer une chaine de Markov sur l'espace d'états des θ dont la loi stationnaire est la loi *a posteriori* selon laquelle nous souhaitons tirer. Il existe plusieurs méthodes pour se déplacer d'un état à l'autre et construire la chaine de Markov, la plus connue étant l'algorithme de Metropolis-Hastings.
Dans Metropolis-Hastings, on se donne un noyau de proposition permettant de transiter d'états en états. A chaque état visité, si la probabilité de l'état candidat suivant est supérieure à celle de l'état courant, alors l'état suivant est visité. Sinon, l'état suivant est visité avec comme probabilité le rapport des probabilités entre les deux états.

Présentons plus formellement la méthode. On se donne un noyau de proposition pour se déplacer sur l'espace des θ. On se donne un point initial θ_0.
Pour se déplacer d'un état θ_t à un état θ_{t+1} :

1) On tire y_{t+1} selon $q(.,\theta_t)$
2) On calcule la probabilité d'acceptation : $\gamma = \min\left(1,\ \frac{\pi(y_{t+1}|\eta(z))q(y_{t+1},\theta_t)}{\pi(\theta_t|\eta(z))q(\theta_t,y_{t+1})}\right)$
3) Si $\gamma = 1$, alors $\theta_{t+1} = y_{t+1}$
   Si $\gamma < 1$, alors $\theta_{t+1} = y_{t+1}$ avec probabilité γ (i.e on tire U une uniforme (0,1) et si U< γ on accepte y_{t+1})
   $\theta_{t+1} = \theta_t$ avec probabilité $1-\gamma$

On recommence ensuite en 1) pour tirer le point suivant jusqu'à obtenir une chaine suffisamment grande.

Calculer le rapport $\frac{\pi(y_{t+1}|\eta(z))q(y_{t+1},\theta_t)}{\pi(\theta_t|\eta(z))q(\theta_t,y_{t+1})}$ suppose d'avoir accès à $f(\eta(z)|\theta)\pi(\theta)$ à une constante multiplicative près. Pouvons-nous calculer la vraisemblance du modèle ransomware ?
Pour un SIR classique, on estime le modèle par rapport à des temps individuels, et on parvient à exprimer la vraisemblance du modèle, à un facteur près, ce qui est suffisant pour utiliser Métropolis-Hastings. Dans notre cas, nous souhaitons utiliser le nombre de victimes et le coût total pour estimer le modèle. θ_I, θ_Ret μ influent sur le coût tandis que α et θ_I influent sur le nombre de victimes. Les caractéristiques des victimes influent elles aussi sur le coût. Calculer la vraisemblance $f(z|\theta)$ revient à se poser la question suivante : sachant θ, quelle est la probabilité d'avoir un tel ensemble d'entreprises infectées avec leurs caractéristiques précises (pays, chiffre d'affaires journalier, secteur d'activité, nombre d'employés, nombre d'ordinateurs, nombre de serveurs, leurs temps infectieux, de réparation et la sévérité de leurs dégâts) engendrant un tel coût ?
On peut séparer le problème en deux étapes : le nombre de victimes et le types de victimes tirées.
La première partie est calculable, puisque c'est l'objet classique des modèles SIR. La seconde est plus compliquée puisqu'elle dépend de la structure de notre portefeuille qui contient un très grand nombre d'assurés aux caractéristiques variées. Pour tout nombre m de victimes, il faudrait :
-construire les m combinaisons possibles d'entreprises parmi notre portefeuille

-regrouper les combinaisons pouvant engendrer le même coût total, c'est-à-dire les combinaisons dont les entreprises vues de manière globale causent potentiellement le même coût total.
-calculer la probabilité d'occurrence de chacun de ces regroupements de combinaisons
Cette seconde étape est nécessaire puisque nous souhaitons estimer les paramètres du modèle lorsque non seulement le nombre de victimes de l'évènement généré est proche de celui de NotPetya mais aussi lorsque les coûts totaux sont proches. Lorsqu'un coût total est renvoyé par le modèle, il y a potentiellement plusieurs combinaisons possibles qui permettent de l'atteindre. Déterminer le nombre de ces combinaisons est nécessaire pour connaître ensuite leur probabilité d'occurrence et ainsi obtenir la vraisemblance du modèle.
Pour utiliser MCMC il faut être en mesure de calculer la vraisemblance à une constante multiplicative près (pour in fine avoir la loi *a posteriori* à une constante multiplicative près), ce qui n'est pas notre cas. Nous n'avons pas trouvé d'expression analytique pour la vraisemblance puisqu'elle dépend d'un espace de grande dimension.
Notre modèle permet de générer des observations synthétiques résultant d'un ransomware. Rappelons que la structure de z_k contenant les observations ainsi générées est la suivante :

$$z_k = \left(\begin{bmatrix} victime_{k,1} \\ \vdots \\ victime_{k,i} \\ \vdots \\ victime_{k,m} \end{bmatrix}, \begin{bmatrix} t_{I\,k,1} \\ \vdots \\ t_{I\,k,i} \\ \vdots \\ t_{I\,k,m} \end{bmatrix}, \begin{bmatrix} t_{R\,k,1} \\ \vdots \\ t_{R\,k,i} \\ \vdots \\ t_{R\,k,m} \end{bmatrix}, \begin{bmatrix} u_{k,1} \\ \vdots \\ u_{k,i} \\ \vdots \\ u_{k,m} \end{bmatrix} \right)$$

Nous nous tournons donc vers la méthode ABC qui permet de passer outre le calcul de la vraisemblance en générant des observations synthétiques via notre modèle. Cela permet de contourner l'absence ou l'observation partielle de données historiques.

3.3.2 Méthode Approximate Bayesian Computation (ABC)

Soit $\theta = (\alpha, \theta_I, \theta_R, \theta_\mu)$ notre vecteur de paramètres aléatoires dont la loi *a posteriori* est à estimer. La méthode ABC classique présentée dans l'article « Approximate Bayesian computational methods » de Jean-Michel MARIN, Pierre PUDLO, Christian P.ROBERT et Robin J.RYDER de 2011 [43] permet de passer outre le calcul de $f(.\,|\theta)$, la vraisemblance du modèle et d'utiliser une transformation statistique η pour comparer les variables simulées selon $f(.\,|\theta)$. Autrement dit, on cherche à générer des évènements semblables (au sens de la transformation η) à NotPetya sur notre portefeuille d'assurés. Voici l'algorithme ABC d'acceptation-rejet provenant de l'article ; les notations coïncident avec notre problème[1] :

[1] A l'exception du domaine de définition D que nous avons noté D_Z

Algorithm 2 Likelihood-free rejection sampler 2

for $i = 1$ to N **do**
  repeat
    Generate $\boldsymbol{\theta}'$ from the prior distribution $\pi(\cdot)$
    Generate $\mathbf{z}$ from the likelihood $f(\cdot|\boldsymbol{\theta}')$
  until $\rho\{\eta(\mathbf{z}), \eta(\mathbf{y})\} \leq \varepsilon$
  set $\boldsymbol{\theta}_i = \boldsymbol{\theta}'$,
end for

where the parameters of the algorithm are

- η, a function on $\mathcal{D}$ defining a statistic which most often is not sufficient,
- $\rho > 0$, a distance on $\eta(\mathcal{D})$,
- $\varepsilon > 0$, a tolerance level.

Figure 22- Algorithme de rejet sans calcul de la vraisemblance, source MARIN et al. (2011)

Cet algorithme a la structure classique d'un algorithme de rejet (rappel en annexe). On veut tirer N simulations de $\theta|y$ afin d'estimer $\pi(\theta|y)$. Tant que le nombre de simulations acceptées est inférieur à N, on tire θ selon $\pi(\theta)$ et on génère ensuite une observation z selon $f(.\,|\theta)$ en prenant θ tout juste tiré. Si la distance $\rho\big(\eta(z), \eta(y)\big)$ est inférieure au seuil de tolérance ε, alors le tirage de θ est accepté. Sinon on recommence l'opération.
Contrairement à un algorithme d'acceptation rejet classique, le critère de sélection ne dépend pas du rapport entre la densité cible et une densité candidate mais de la distance entre $\eta(z)$ simulé et la cible $\eta(y)$.

Nous résumons les explications de l'article, quant à l'intuition derrière la méthode ABC basée sur cet algorithme de rejet.
Notations :
$\mathbb{1}_E(.)$ est la fonction indicatrice pour l'ensemble E.
$A_{\varepsilon,y} = \{z \in D \text{ tel que } \rho\big(\eta(z), \eta(y)\big) \leq \varepsilon\}$ l'ensemble des points z de D pour lesquels $\eta(z)$est dans un voisinage de $\eta(y)$ de taille ε pour la métrique ρ.
$\eta(.)$ est une transformation statistique permettant de comparer les simulations z et la cible y avant de pouvoir appliquer la métrique ρ. Pour avoir une bonne estimation de $\pi(\theta|y)$, $\eta(.)$ doit contenir suffisamment d'informations sur les simulations z, tout en étant de dimension la plus faible possible pour éviter des problèmes de dimensions lors du calcul de la distance ρ.
L'idée est donc de regarder la distribution des θ amenant notre modèle à être suffisamment proche de y afin d'estimer $\pi(\theta|y)$.
L'échantillon de θ fourni par l'algorithme précédent suit en réalité la loi marginale en z de la distribution jointe suivante :

$$\pi_\varepsilon(\theta, z|y) = \frac{\pi(\theta) f(z\,|\theta) \mathbb{1}_{A_{\varepsilon,y}}(z)}{\int_{A_{\varepsilon,y}\times H} f(z|\,\theta)\pi(\theta) dz d\theta}$$

Où $\pi_\varepsilon(\theta, z|y)$ est la loi du couple (θ, z) retreinte à $A_{\varepsilon,y}$
$\int_{A_{\varepsilon,y}\times\theta} f(z|\,\theta)\pi(\theta) d\theta dz$ est la probabilité que (θ, z) soit dans $A_{\varepsilon,y} \times H$.
On intègre $\pi_\varepsilon(\theta, z|y)$ selon z pour avoir $\pi_\varepsilon(\theta|y)$. On suppose ensuite que $\pi_\varepsilon(\theta|y) \approx \pi(\theta|y)$.
L'idée derrière la méthode ABC est que la statistique $\eta(.)$ couplée à une tolérance ε faible donne une bonne approximation de la loi *a posteriori*. L'idéal serait que $\eta(.)$ soit une statistique exhaustive, mais

cette condition est rarement vérifiée en pratique. Nous allons voir que dans notre cas, le choix de la statistique $\eta(.)$ s'impose naturellement.

La solution que nous proposons est de construire une transformation $\eta(.)$ de Z dont l'observation réelle soit connue pour NotPetya. Pour NotPetya, on se basera sur une transformation statistique $\eta(Z)$ utilisant h (afin d'incorporer toutes nos connaissances acquises *a priori*) pour calculer le coût total de l'évènement et donnant aussi le nombre de victimes. Dans notre algorithme, la comparaison de $\eta(z)$ et $\eta(y)$ se fait sous les mêmes conditions que NotPetya (i.e. en fixant les hyper-paramètres)

- **Construction de la transformation η**

Adaptons la méthode à notre problème. y est dans notre cas la réalisation de Z correspondant à NotPetya. Nous voudrions donc connaître la loi de θ lorsque Z est proche de y. Autrement dit, on veut $\pi(\theta|Z=y)$, ce qui est un abus de notation puisque est Z une variable aléatoire continue. Nous noterons simplement $\pi(\theta|y)$. Un obstacle se dresse ici puisque nous n'avons pas accès directement à y (qui contiendrait les observations complètes de NotPetya à savoir le profil des victimes, le taux de transmission, temps infectieux et de réparation, sévérités etc…). Avec la méthode ABC nous sommes en mesure de passer outre cet obstacle : $\pi(\theta|y)$ est approchée par $\pi(\theta|\eta(y))$. On fait une approximation en estimant la loi de θ non pas lorsque Z est proche de y mais lorsque $\eta(Z)$ est proche de $\eta(y)$. Explicitons maintenant notre fonction $\eta(.)$.
Notons g la fonction définie sur D_Z et à valeurs dans $\mathbb{R}^+ \times \mathbb{R}^+$ telle que :

$$g(z_k) = (\textit{nombre total de victimes de } z_k, \textit{perte économique totale de } z_k)$$

Remarquons que la fonction h intervient dans le calcul de la seconde coordonnée de $g(z_k)$.
En effet : *perte économique totale de* $z_k = \sum_{i=0}^{m} h(z_{k,i})$
On se donne un point cible $g(y) = (200\ ,\ 0.874 \times 10^9)$, en accord avec l'hypothèse vi).
Il est préférable de normaliser *les* $g(z_k)$ pour éviter les problèmes d'échelle lors du calcul de la distance ρ. On note $\eta(z_k)$ la normalisation de $g(z_k)$.
Ainsi, la construction de $\eta(.)$ s'est naturellement imposée à nous. Cette fonction permet d'utiliser toutes les connaissances que nous avons sur NotPetya : le coût total, le nombre total de victimes et la fonction de coût h dont la structure prend aussi en compte les connaissances que nous avons acquises. Nous ne sommes pas en mesure de vérifier que $\eta(.)$ soit une statistique exhaustive (et elle ne l'est sans doute pas), mais nous avons de toute façon fait en sorte que $\eta(.)$ contienne le plus d'information possible.
On définit enfin ρ comme la distance L^2 pondérée.
$\forall (x,y) \in \mathbb{R}^2 \times \mathbb{R}^2$ et $(p_1, p_2) \in \mathbb{R} \times \mathbb{R}$, tels que $p_1 + p_2 = 1$,
on a $\rho(x,y) = \sqrt[2]{p_1(x_1 - y_1)^2 + p_2(x_2 - y_2)^2}$
et $\eta(z_k) = (\textit{nombre total de victimes de } z_k \textit{ normalisé}, \textit{perte économique totale de } z_k \textit{normalisée})$
Nous accordons plus d'importance au coût de l'évènement et décidons de lui donner un poids plus important dans la métrique ρ.
Nous prendrons $p_1 = 0.3$ et $p_2 = (1 - p_1) = 0.7$
Sélectionner une boule au lieu d'un cube nous évitera d'avoir les deux conditions de sélection saturées. Ainsi lorsqu'une composante d'un point accepté est éloignée de la cible, l'autre composante est nécessairement plus proche pour que la simulation soit acceptée.

La méthode soulève la question du choix du seuil ε permettant de choisir les « bonnes » simulations. Ce seuil peut être soit une valeur fixe, soit un quantile des distances entre les simulations et la cible [43]. Le choix d'un quantile des distances comme seuil de sélection a l'avantage de fixer à l'avance le

nombre de simulations nécessaires pour obtenir un échantillon de taille donnée. La question qui se pose alors est comment déterminer l'ordre du quantile. Nous aborderons plus en détails cette problématique lors des estimations.

Conclusion : Nous avons donc montré que le recours au cadre bayésien et plus particulièrement à la méthode ABC prenait ici tout son sens. Contrairement à la méthode MCMC, la méthode ABC ne requiert pas le calcul explicite de $f(.|\theta)$ mais suppose uniquement de savoir générer selon $f(.|\theta)$. Cette facilité de mise en œuvre ne vient pas sans un coût : le nombre de simulations nécessaires élevé induisant un temps de calcul important. Si on avait accès directement à $f(.|\theta)$, il serait préférable d'utiliser une méthode MCMC qui est plus rapide. Nous allons maintenant estimer les lois *a posteriori* pour 3 modèles se différenciant uniquement par les loi *a priori* données aux paramètres. Nous étudierons ensuite les avantages et inconvénients présentés par chacun des modèles avant d'un choisir un que nous utiliserons pour simuler la perte assurée

3.3.3 Premier modèle

Nous présentons ici les résultats de notre première approche. Nous détaillons dans un premier temps les choix de lois *a priori* avant d'expliquer notre procédure pour valider l'emploi de la méthode ABC et d'analyser l'échantillon accepté.

3.3.3.1 Hypothèses du modèle

Comme évoqué au début de cette partie, trois variables sont fixées (le coût de la rançon est déterministe et vaut 600 dollars, le temps avant le patch est fixé à 24 heures, la proportion de vulnérables est fixée à 46.77%).
Nos inconnues restantes sont les lois de α, θ_I , $\theta_R$et θ_μ.
Pour cette première approche d'estimation, nous supposons les lois suivantes pour les paramètres :

Paramètre	Loi *a priori*
α	$U(0,1)$
θ_I	Constante égale à $\frac{1}{10}$
θ_R	Constante égale $\frac{1}{20}$
θ_μ	Constante égale à 0.9

Tableau 36- Lois a priori des paramètres pour le premier modèle

Nous connaissons uniquement le support du taux de transmission α et prenons par conséquent une loi uniforme sur [0,1] comme loi *a priori* pour α.
Pour proposer un premier modèle simple, nous avons fixé les paramètres θ_I , θ_R et θ_μ.
Expliquons les choix des valeurs choisies. D'après Wired, Maersk a mis plus de 2 heures pour déconnecter totalement ses systèmes contaminés des réseaux et 10 jours pour reprendre une activité normale. L'article décrit la gestion de crise de Maersk comme étant particulièrement rapide, nous prenons donc une valeur de 10 heures nettement supérieure comme moyenne du temps infectieux (on rappelle que pour une variable T suivant une loi exponentielle de paramètre λ, $\mathbb{E}(T) = \frac{1}{\lambda}$ et $\mathbb{V}(T) = \frac{1}{\lambda^2}$). Pour les temps de réparation, une relation de proportionnalité entre les temps de réparation totaux

et la reprise d'activité de Maersk pourrait être trop optimistes : nous ne souhaitons donc pas estimer θ_R de manière fréquentiste sur ce très petit échantillon. Selon une étude interne à AXA, un évènement grave entraine en général une indisponibilité des systèmes informatiques pour une durée de 10 jours contre 30 jours pour un évènement extrême. Nous situons NotPetya entre ces deux catégories d'évènements et prenons 20 jours comme moyenne. Nous avons introduit ici beaucoup de jugements subjectifs. Nous rendrons les paramètres de ces deux lois aléatoires pour le second modèle (3.3.4).

Pour la sévérité μ on se donne une variable aléatoire uniforme entre 0.1 et 0.9. Nous avons pris $\theta_\mu = 0.9$ car NotPetya a eu des impacts pouvant être de très forte intensité selon les victimes : nous voulons donc conserver une grande amplitude de sévérité entre les assurés touchés.

Les hypothèses faites ici restreignent le paramètre aléatoire θ à α.
En effet, on a $\theta = (\alpha \sim U(0,1)\ , \theta_I = \frac{1}{10}, \theta_R = \frac{1}{20}, \theta_\mu = 0.9)$.
Pour ce premier modèle, nous avons incorporé beaucoup de jugement d'expert. Seul le taux de transmission α pour lequel nous n'avons à priori aucune information est rendu aléatoire via un *a priori* non informatif. Les autres paramètres ont été fixés via des hypothèses construites à partir de jugements d'experts et de sources d'information diverses. Via l'étude des simulations obtenues à partir de ce modèle, nous souhaitons donc vérifier que nos hypothèses et sources d'informations décrivent bien l'évènement cible NotPetya et parviennent par conséquent à l'approcher.

3.3.3.2 Validation de la méthode

Nous souhaitons obtenir 500 réalisations de $\theta|y$ avec l'algorithme présenté en 3.3.2.3).
Afin d'obtenir nos 500 réalisations de $\theta|y$, nous choisissons de prendre les 2.5% des simulations les plus proches de notre cible $\eta(y)$ parmi 20 000 simulations. ε est donc ici choisi comme le quantile à 2.5% de nos 20 000 simulations.
Nous souhaitons vérifier que la méthode appliquée à notre modèle soit robuste sur des données synthétiques avant d'utiliser notre méthode sur la vrai cible : NotPetya. Pour cela, on souhaite contrôler que les θ acceptés soient potentiellement issus de la loi *a posteriori* et qu'un autre facteur de risque n'influe pas sur la répartition des $\eta(z_k)$.
La validation du modèle repose sur le principe suivant : pour une réalisation z obtenue on calcule $\eta(z_k)$ et on vérifie si l'ensemble des θ à l'origine d'un voisinage de $\eta(z_k)$ contient le θ qui a permis d'obtenir z_k. Plus précisément, on procède au test suivant : pour chaque $\eta(z_k)$ on regarde les 2.5% des 19 999 simulations les plus proches pour la métrique ρ. Si le θ appartient bien à l'ensemble des θ autour de $\eta(z_k)$ alors nous dirons que la méthode est valide : θ est potentiellement une réalisation de la loi de θ autour de $\eta(z_k)$. Les observations synthétiques générées vont tour à tour servir de cible à l'algorithme ABC. On affecte 1 quand le test est validé et 0 sinon. La validité de la méthode est ensuite obtenue en prenant la moyenne des tests obtenus sur chaque $\eta(z_k)$. Si ce score de validité est élevé pour des cibles fictives, nous pourrons passer à la cible réelle : NotPetya.

Pour ce premier modèle, θ est constitué du seul paramètre α, la validation revient donc à étudier si α appartient à l'intervalle ayant comme bornes le maximum et le minimum des α à l'origine de la boule autour de $\eta(z_k)$. Ici nous choisissons de prendre le maximum et le minimum des θ comme intervalle test pour autoriser une grande volatilité de θ. En effet, notre objectif final est de construire des évènements proches de NotPetya mais pas totalement similaires. On veut donc choisir un seuil permettant d'accepter un ensemble de θ assez étendu autours du maximum *a posteriori* (MAP). On vérifie donc que le support de la loi *a posteriori* contienne bien le θ à l'origine de l'observation.

Sur nos 20 000 simulations, 19 964 vérifient le test précédent. La méthode est donc valide à 99.82%.
Si on avait pris un quantile à 0.5% au lieu d'un quantile à 2.5%, alors le nombre de simulations vérifiant le test diminue à 19 783. La méthode serait alors valide à 98.9%.
On pourrait penser qu'en réduisant la valeur du seuil d'acceptation ε on augmenterait la précision de l'estimation de la loi *a posteriori* de θ. Mais en diminuant le seuil sans augmenter le nombre de simulations, on risque de se priver de la vraie valeur de θ puisque l'échantillon sélectionné approche trop fortement le MAP. La possibilité d'avoir un θ à l'origine de la simulation qui puisse être éloigné du MAP provient de la volatilité induite par d'autres paramètres du modèle et de l'hétérogénéité de notre portefeuille d'assurés. Pour augmenter la précision, il faut diminuer le seuil d'acceptation ε tout en augmentant le nombre de simulations.
Le quantile optimal permettant de définir le seuil d'acceptation n'est pas celui qui donne 100% de validité au test précédent, sinon 1 serait solution et tous les θ simulés seraient acceptés. Le choix du quantile est une question importante. Ce seuil de sélection doit permettre d'avoir un ensemble assez petit autour de la cible pour bien estimer la loi *a posteriori*, sans pour autant être trop petit sous peine de priver la loi *a posteriori* de ses réalisations éloignées du MAP.
Un critère de sélection à l'œil nu pourrait être de sélectionner le premier quantile après lequel le gain de validité de la méthode devient marginal. Ce critère permet de maximiser la validité de notre méthode tout en minimisant la taille de l'échantillon accepté. Nous avons tiré aléatoirement 10 000 points et avons tracé le pourcentage de validité de la méthode en fonction d'une grille de quantiles à 0.1, 0.2, 0.4, 1, 2.5, 5, 10 pourcents :

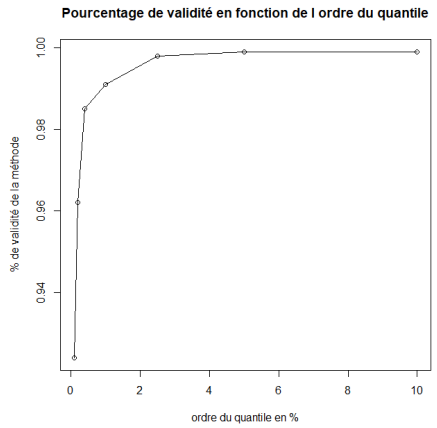


Figure 23 - Choix de l'ordre du quantile déterminant le seuil ε

En suivant cette méthode, on voit que notre choix initial de 2.5% est assez bien choisi. Une méthode plus précise mais bien plus couteuse serait de se donner un pas régulier d'ordres de quantiles et de calculer l'accroissement de validité entre deux points. On sélectionnerait ainsi l'ordre du quantile précédent un accroissement négligeable.

3.3.3.3 Étude des simulations

Regardons maintenant nos 20 000 simulations par rapport à la cible réelle.
Le graphique suivant présente les résultats des simulations dans le plan (Nombre total de victimes normalisé, Coût total normalisé). On trace $\eta(z_k)$ pour k allant de 1 à 20 000 et la cible $\eta(y)$ en rouge.

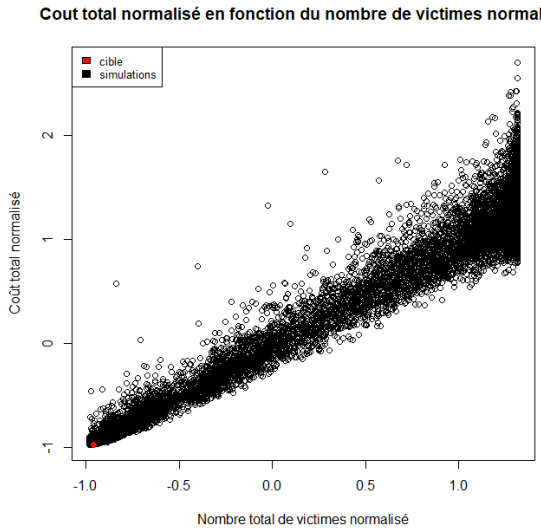


Figure 24 - Graphique des 20 000 transformations $\boldsymbol{\eta(z_k)}$ et la cible $\boldsymbol{\eta(y)}$

On observe une relation linéaire croissante entre le nombre de victimes et le coût. Cette relation est logique : plus le nombre de victimes augmente, plus le coût est important.

On remarque que notre cible $\eta(y)$ correspond à un faible nombre de victimes et un faible coût économique par rapport à l'ensemble des simulations : la cible a pour coordonnées (-0.97, -0.96).

Le nombre de victimes dépend de α et des temps infectieux simulés selon T_I tandis que le coût total dépend du nombre de victimes (et donc là aussi de α et des temps infectieux simulés selon T_I) mais aussi des temps de réparation simulés selon T_R, des sévérités simulées selon μ , des entreprises tirées et de h. Pour les deux variables les corrélations avec α sont positives (0.92 pour le coût et 0.93 pour le nombre de victimes) mais on s'attend à ce que α influence d'avantage le nombre de victimes que le coût. Afin d'étudier la dépendance de ce modèle à α, on trace le coût total et le nombre de victimes en fonction de α.

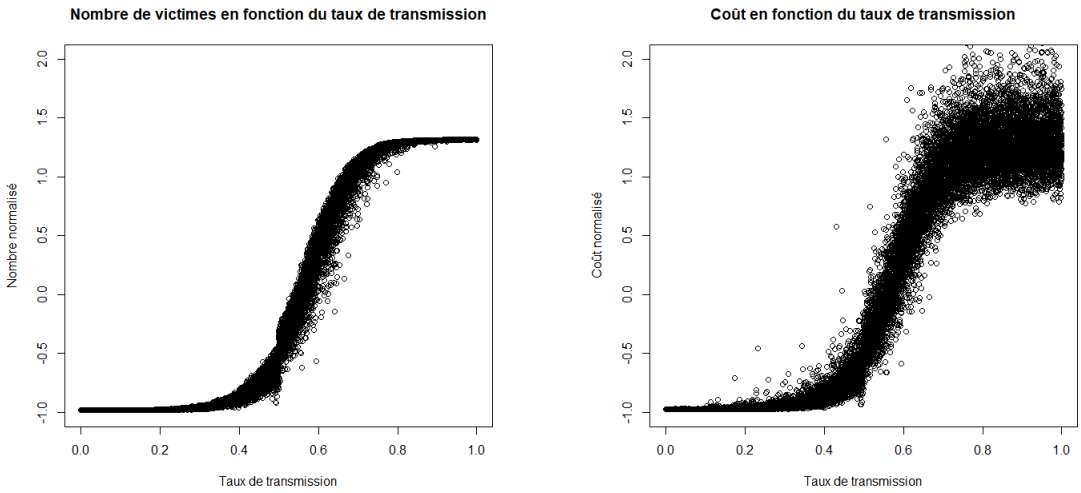


Figure 25- Influence de α sur le coût et le nombre de victimes

Le premier graphique présente des points beaucoup moins dispersés que le second. On regarde les variations des valeurs prises par le coût et le nombre de victimes selon α et on reporte les résultats suivants[1] :

α	Max victimes	Min victimes	amplitude	Ecart type	Max coût	Min coût	amplitude	Ecart type
0.2	-0.977	-0.988	0.010	0.002	-0.882	-0.978	0.096	0.008
0.4	-0.766	-0.949	0.183	0.036	-0.088	-0.961	0.873	0.070
0.6	0.773	-0.390	1.163	0.195	1.869	-0.469	2.337	0.278
0.8	1.302	1.084	0.218	0.019	2.073	0.685	1.388	0.222

Tableau 37- Dispersions du coût et du nombre de victimes en fonction de α

Le tableau précédent a été obtenu en prenant une fenêtre de 0.04 centrée en α.

α	$\frac{\textit{Ecart type Coût}}{\textit{Ecart type Victimes}}$	$\frac{\textit{Amplitude Coût}}{\textit{Amplitude Victimes}}$
0.2	4.295	9.264
0.4	1.948	4.776
0.6	1.427	2.011
0.8	11.938	6.367

Tableau 38- Analyse des résultats de dispersion

Pour chaque valeur de α, l'amplitude et l'écart-type du coût sont au moins 1.4 fois et 2 fois plus élevés que l'amplitude et l'écart-type du nombre de victimes. α influence donc d'avantage le nombre de victimes que le coût. Pour le coût, ce sont les temps de réparation, les sévérités et les entreprises tirées qui introduisent une variabilité supplémentaire.

Nous nous focalisons maintenant sur les simulations acceptées par notre algorithme de rejet.
Le quantile à 2.5% de nos 20 000 simulations est $\varepsilon = 0.00639$

[1] Nous présentons les valeurs centrées réduites afin d'observer la variance du coût et du nombre de victimes induite par α et annuler l'effet provenant de la variance propre à chacune de ces deux variables. Nous donnons ici les constantes de normalisation permettant de retrouver les valeurs d'origine : écart-type du coût : 80 milliards €; moyenne du coût : 70 milliards €; écart-type du nombre de victimes : 16 841 , moyenne du nombre de victimes : 16 157

Pour le graphique suivant, nous avons réduit la fenêtre au carré $[-1,-0.8] \times [-1,-0.8]$ et tracé en vert les simulations acceptées par l'algorithme de rejet et en noir celles rejetées. Notre cible est toujours représentée par un point rouge.

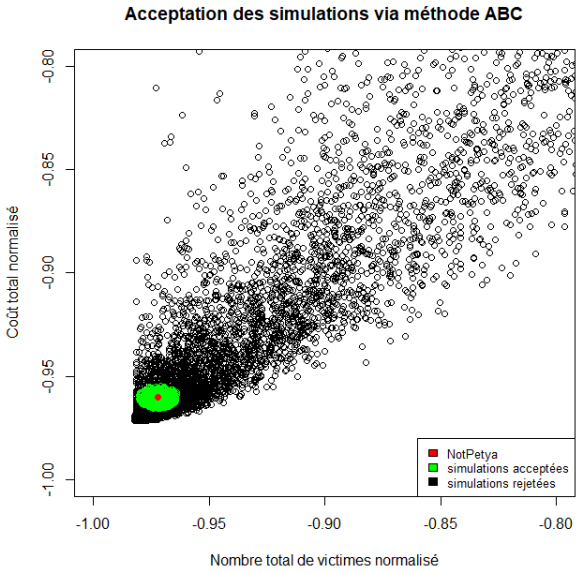


Figure 26 - Zone d'acceptation de la méthode ABC

Les simulations acceptées sont dans une boule centrée en notre cible $\eta(y)$ et de taille ε pour la métrique ρ. Comme le poids associé au nombre de victimes est moins important, nous avons une boule étirée par rapport aux abscisses : nous acceptons bien une plus grande amplitude de valeurs pour le nombre de victimes que pour le coût total de l'évènement.

3.3.3.4 Analyse de l'échantillon accepté

θ est ici restreint à α. On obtient $\pi(\theta|y)$ en regardant la loi de α sur notre échantillon accepté.

- **Taux de transmission α**

Regardons l'histogramme des réalisations de α pour avoir une idée de la loi *a posteriori*. On estimera ensuite une loi paramétrique sur cet échantillon pour obtenir $\pi(\theta|y)$.

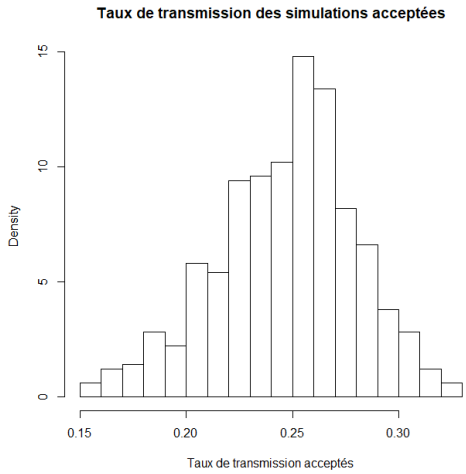


Figure 27- Histogramme du taux de transmission α des simulations acceptées

On obtient une moyenne empirique de 0.25. Cette loi est à première vue asymétrique avec une queue de distribution plus fine à droite. Le coefficient d'asymétrie (skewness) est négatif (-0.33) ce qui confirme notre observation faite à l'œil nu. Nous éliminons donc la loi normale puisque cette dernière est symétrique. Nous éliminons aussi la loi log-normale et gamma puisque leurs skewness sont positifs[1]. La loi de weibull permet d'avoir un skewness positif ou négatif selon la valeur de ses paramètres. Nous essayons donc de calibrer une loi de Weibull sur notre échantillon. Pour ce faire nous utilisons le package « fitdistrplus » disponible sur R. (En annexe une capture d'écran du code utilisé).

L'estimation d'une loi de Weibull par maximisation de la vraisemblance donne 8.65 comme paramètre de forme et 0.26 comme paramètre d'échelle. Le test de Kolmogorov Smirnov [2] renvoie 0.55 comme p-valeur, : l'hypothèse H0 « l'échantillon suit une loi de Weibull(8.65, 0.26) » est acceptée au seuil de confiance 5%. Le graphique suivant confirme de manière visuelle l'adéquation entre l'échantillon accepté et une loi de Weibull.

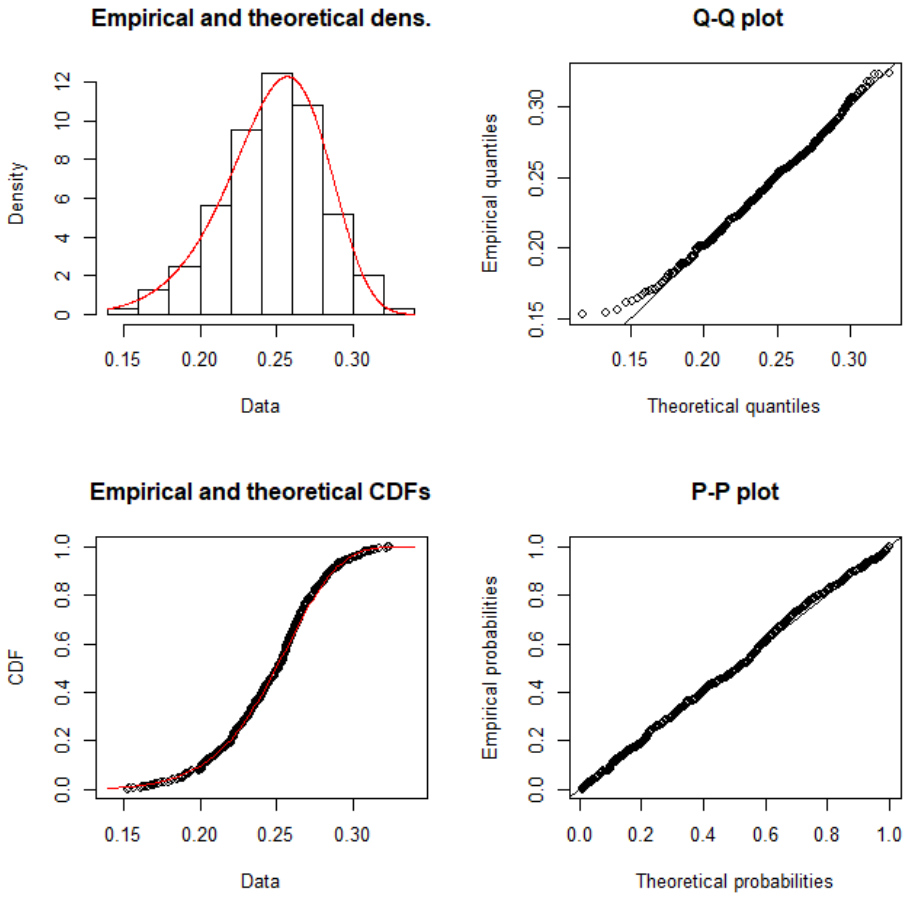


Figure 28- Estimation d'une loi de Weibull sur l'échantillon

La densité de notre loi de Weibull(8.65, 0.26) adossée à l'histogramme semble bien coller aux données, de même pour les fonctions de répartition et le P-P plot qui permettent de voir que le centre de la distribution est bien en adéquation avec une loi de Weibull. Avec le Q-Q plot on note que le poids des faibles valeurs est légèrement sous-estimé par la loi théorique tandis que la queue de distribution empirique est en adéquation avec la queue théorique. Ceci pourrait provoquer une légère tendance à

[1] Des rappels sur les lois paramétriques usuelles sont fournis en Annexe.

[2] Le test de Kolmogorov Smirnov est rappelé en Annexe. Il permet de tester l'adéquation de la fonction de répartition théorique à la fonction de répartition empirique grâce à l'étude du Sup de la valeur absolue des écarts entre ces deux fonctions qui est une loi tabulée.

négliger des petits évènements si nous conservons cette estimation de la loi *a posteriori* pour effectuer nos simulations.

- **Temps infectieux, temps de réparation et sévérité**

Les temps infectieux, de réparation et de sévérité ont été tirés selon la même loi pour chaque victime à chaque simulation d'une attaque puisque nous avions fixé θ_I, θ_R et θ_μ. On n'observe donc aucun changement dans ces lois : l'échantillon accepté possède les mêmes lois de sévérité, de temps infectieux et de temps de réparation que celles que nous avions fixées.

- **Nombre total de victimes et coût total**

Regardons de plus près ces variables non normalisées

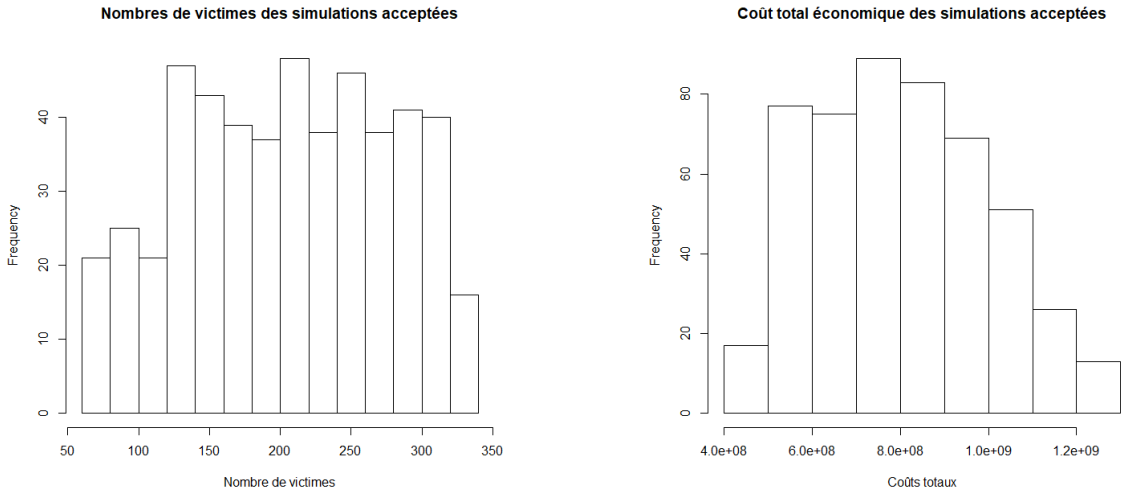


Figure 29-Histogrammes du nombre de victimes et du coût total de l'échantillon accepté

Notre cible correspond à 10% de 8.74 milliards d'euros donc à 8.74×10^8 euros, soit 874 millions. Les simulations sélectionnées ne sont pas centrées en 874 millions : on a une perte totale moyenne d'environ 803 millions de euros pour nos simulation acceptées. Cependant, la fenêtre d'acceptation est bien centrée en 874 millions puisque les simulations acceptées vont de 468 millions d'euros à 1.27 milliards d'euros. On a donc plus de simulations sélectionnées dont la perte est inférieure à la cible, ce qui fait diminuer la moyenne de l'échantillon accepté.
Pour le nombre de victimes, nous avions 200 comme cible et obtenons ici une moyenne d'environ 204 victimes et des valeurs comprises entre 61 et 337.

- **Coût par police**

Nous regardons maintenant le coût économique individuel pour vérifier si l'amplitude de coûts simulés par notre fonction h correspond à nos attentes.

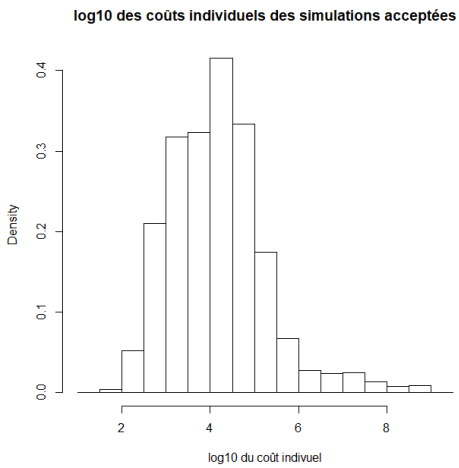


Figure 30 - log10 des coûts individuels des simulations acceptées

Sur nos 500 simulations acceptées, on obtient un coût par police médian de 13 000 euros et une moyenne de 3.9 millions d'euros. Cet écart entre la médiane et la moyenne provient des très grandes valeurs prises par h sur certaines polices.
Les coûts supérieurs à 1 million d'euros représentent 5% des coûts individuels, ceux supérieurs à 100 millions représentent 0.7% et ceux supérieurs à 300 millions d'euros représentent 0.45%. Notre fonction h permet d'avoir une grande amplitude dans les coûts simulés et nous sommes assez proche de la répartition du coût décrite en 3.2.4).

Conclusion : Nous arrivons donc à reproduire des évènements ayant un impact proche de NotPetya et ceci en ayant émis des hypothèses fortes sur nos trois variables de temps infectieux, temps de réparation et sévérité. Ce modèle possède des lois paramétriques simples pour ses paramètres et peut donc être facilement mis en œuvre. Au cours de l'étude de ce premier modèle, nous avons pu nous familiariser avec la méthode ABC et son principal enjeu : le choix du seuil d'acceptation des simulations. Ce premier modèle est encourageant puisque les informations sur NotPetya que nous avons utilisées *a priori* pour la construction de la fonction de coût h et pour le choix des valeurs de θ_I, θ_R et θ_μ nous permettent d'atteindre la cible avec ce modèle. Nous aurions pu avoir une cible non approchée par nos simulations. Cela signifierait que la cible n'est pas issue du processus que nous simulons et par conséquent que nos choix de modélisation sont quelque part erronés. Par exemple, en considérant une cible ayant comme coût total 8 milliards de dollars et causé environ 100 000 victimes nous constatons que le point associé est hors d'atteinte pour ce modèle. Cet exemple n'est pas anodin puisqu'il s'agit de WannaCry.

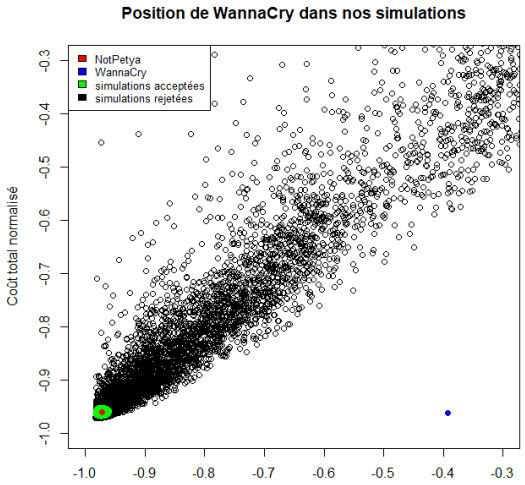


Figure 31 - WannaCry par rapport aux simulations du premier modèle

3.3.4 Second modèle

Nous souhaitons voir ici s'il est possible d'approcher encore mieux notre cible en introduisant de l'aléa supplémentaire sur certains paramètres du modèle.

3.3.4.1 Hypothèses du modèle

Pour le premier modèle nous avions totalement fixé les paramètres θ_I et θ_R en étudiant les moyennes des temps infectieux et des temps de réparation en faisant appel à des articles, des études et notre jugement. Nous rendons ici aléatoire ces paramètres afin d'étudier d'une part si le modèle approche mieux la cible et d'autre part si nos choix pour le premier modèle étaient cohérents et les seuls possibles pour approcher la cible.

Voici le tableau des lois que nous donnons a priori pour les paramètres du modèle :

Paramètre	Loi *a priori*
α	$U(0,1)$
θ_I	$\frac{1}{\theta_I} \sim U(2,24)$
θ_R	$\frac{1}{\theta_R} \sim U(10,30)$
θ_μ	Constante égale à 0.9

Tableau 39 - Lois a priori des paramètres pour la second modèle

Pour θ_I on a très peu d'information. On décide donc que la moyenne du temps infectieux vit simplement dans l'intervalle [2,24]. Pour θ_R, notre étude AXA nous indique qu'une attaque grave engendre en moyenne 10 jours d'interruption d'activité contre 30 jours pour une attaque extrême. Nous faisons donc vivre l'espérance du temps de réparation dans l'intervalle [10,30].

Dans les deux cas, nous ne privilégions pas de valeurs au sein de ces intervalles. On souhaite donc que l'espérance de nos lois exponentielles vive uniformément dans un intervalle $[b,c]$ avec $1 < b < c$.

Si $\frac{1}{\theta} \sim U(b,c)$ alors que suit θ ? La fonction $x \mapsto \frac{1}{x}$ est continue et strictement décroissante sur $[b,c]$ donc bijective sur $[b,c]$. On peut donc appliquer la formule du changement de variables. Soit $\varphi: \mathbb{R} \to \mathbb{R}$ mesurable bornée, on a :

$$\mathbb{E}[\varphi(\theta)] = \int_b^c \frac{\varphi(\theta)}{c-b} d\frac{1}{\theta} = \int_{\frac{1}{c}}^{\frac{1}{b}} \frac{\varphi(\theta)}{c-b} \left|\frac{-1}{\theta^2}\right| d\theta = \int_{\frac{1}{c}}^{\frac{1}{b}} \frac{\varphi(\theta)}{c-b} \frac{1}{\theta^2} d\theta$$

On note $l(b,c)$ la loi de θ dont la densité est $\frac{1}{(c-b)\theta^2} \mathbb{1}_{[\frac{1}{c},\frac{1}{b}]}(\theta)$ qui est continue et strictement décroissante sur $[\frac{1}{c},\frac{1}{b}]$. Pour simuler selon cette densité nous pouvons donc utiliser la méthode d'inversion. On note F_θ la fonction de répartition de θ. Par définition, $F_\theta(x) = P(\theta \leq x) = \int_{\frac{1}{c}}^{x} \frac{1}{(c-b)\theta^2} d\theta = \frac{c-\frac{1}{x}}{c-b}$. En inversant cette fonction on obtient : $F_\theta^{-1}(x) = \frac{1}{c-x(c-b)}$.

Pour simuler selon $l(a,b)$, il suffit de prendre U~$U(0,1)$ et de tirer $\theta = F_\theta^{-1}(U)$ (la preuve est disponible en annexe).
Pour ce second modèle, nous simulerons donc θ_I selon $l(2,24)$ et θ_R selon l(10,30).
Ainsi au sein de nos simulations, les espérances de temps infectieux et de réparation seront uniformément distribuées sur [2,24] et [10,30] respectivement. Nous conservons une loi uniforme pour le taux de transmission α et θ_μ fixé.

Pour ce second modèle les composantes de θ sont indépendantes et on a les lois marginales *a priori* suivantes :

$$\theta = (\alpha\text{~}U[0,1], \theta_I\text{~}l(2,24)\ , \theta_R\text{~}l(10,30), \theta_\mu = 0.9)$$

3.3.4.2 Validation de la méthode

Pour des questions de gestion de la mémoire, nous avons stocké uniquement les simulations pour lesquels le coût total était inférieur à 5 milliards d'euros. Nous avons au total stocké un échantillon tronqué contenant uniquement 37 972 simulations sur 100 000 simulations totales. Nous déterminons l'ordre des quantiles par rapport aux 100 000 simulations totales, en admettant que l'échantillon non stocké n'intervient pas sur la valeur du quantile.
Nous réitérons la méthode de validation présentée en 3.3.3.2). Pour chaque simulation z_k nous regardons si θ_k à l'origine de z_k appartient à l'ensemble des θ à l'origine d'une boule centrée en $\eta(z_k)$ de rayon le quantile à q% des distances ρ entre les autres points simulés et $\eta(z_k)$. On assigne 1 si ce test est vérifié et zéro sinon. On calcule ensuite le pourcentage de validité engendré par q.
Nous avons tiré aléatoirement 10 000 points et tracé le pourcentage de validité de la méthode en fonction d'une grille de quantiles à 0.1, 0.2, 0.4, 1, 2.5 et 4 pourcents :

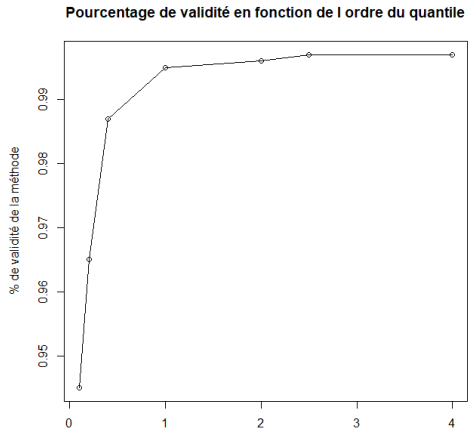


Figure 32-Choix de l'ordre du quantile déterminant le seuil ε

On obtient respectivement des scores de validité de 94.5, 96.5, 98.7, 99.5, 99.6, 99.7 et 99.7 pourcents.
Selon le critère évoqué en 3.3.3.3) nous choisissons ici un quantile à 1%.
La méthode étant valide, nous pouvons donc regarder la boule autours de notre cible réelle.

3.3.4.3 Premières 10 000 simulations

Pour des questions de mémoire, nous stockons uniquement les évènements dont le coût total économique est inférieur à 5 milliards d'euros. Les constantes de normalisation sont en revanche calculées sur l'ensemble des simulations.

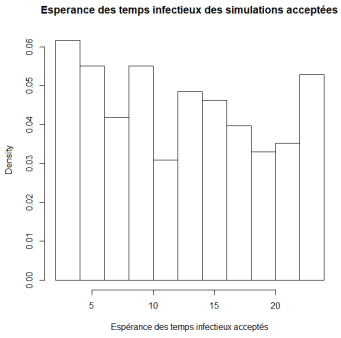
Nous avons dans un premier temps étudié seulement 10 000 simulations afin de vérifier que la cible puisse être assez souvent atteinte avec la volatilité supplémentaire que nous avons ajoutée aux paramètres. Parmi ces 10 000 simulations nous en avons stocké uniquement 3819.

Pour comparer ce modèle au précédent, on calcule le quantile à 2.5% des 10 000 simulations (qui correspond à un quantile à 6.55% des 3 819 simulations stockées en admettant que celles non stockées sont suffisamment éloignées pour ne pas influencer la valeur du quantile). Il vaut 0.0042 contre 0.00639 pour la première simulation. Comme la boule sélectionnée a une norme plus petite pour la seconde approche, cela signifie que nous sommes plus proches de la cible pour cette seconde approche d' estimation.

Le taux de transmission et le coût ont une corrélation de 0.84 contre 0. 92 précédemment tandis que le taux de transmission et le nombre de victimes ont une corrélation de 0.91 contre 0.93 précédemment. L'introduction de variables aléatoires supplémentaires augmente la volatilité des simulations, ce qui diminue la corrélation entre le taux de transmission et le nombre de victimes et le coût total économique. Nous allons sans doute nécessiter plus de simulations pour calibrer correctement les paramètres.

Lorsqu'on s'intéresse aux taux de transmission acceptés, on a une moyenne empirique de 0.25 qui est identique à celle trouvée lors du premier estimation. Cependant, nous avons une loi qui est cette fois-ci de skewness positif donc de queue plus fine à gauche qu'à droite.

Pour les sévérités, comme pour le premier modèle la loi ne change pas car aucun paramètre n'est rendu aléatoire.
Pour les temps infectieux la moyenne des temps acceptés semble peu à peu prendre plus de poids sur la partie inférieure de l'intervalle donné *a priori*.
En ce qui concerne le temps de réparation, la moyenne des temps acceptées semble quant à elle prendre légèrement plus de poids sur la partie supérieure de l'intervalle donné *a priori.*



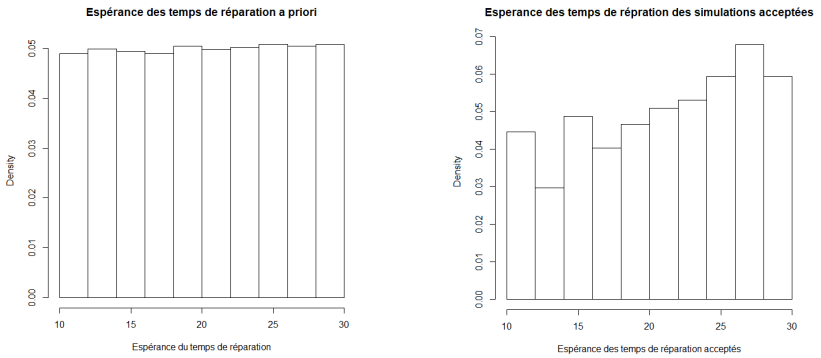


Figure 33 - Espérance des temps infectieux et de réparation a priori et a posteriori pour 10 000 simulations

Les conjectures que nous venons de faire sont à prendre avec précaution puisque nous avons pour l'instant un faible nombre de simulations. Nous allons maintenant effectuer davantage de simulations pour étudier comment évoluent les lois *a posteriori* de nos paramètres.

3.3.4.4 Analyse de l'échantillon accepté

Passons maintenant à 100 000 simulations. Nous avions choisi un quantile optimal d'ordre 1%, nous obtenons donc 1 000 simulations acceptées. Ce quantile vaut 0.0029, ce qui confirme la tendance observée sur les 10 000 premières simulations, à savoir que nous approchons mieux NotPetya avec ce modèle qu'avec le premier. En traçant la zone d'acceptation on obtient donc une boule plus petite :

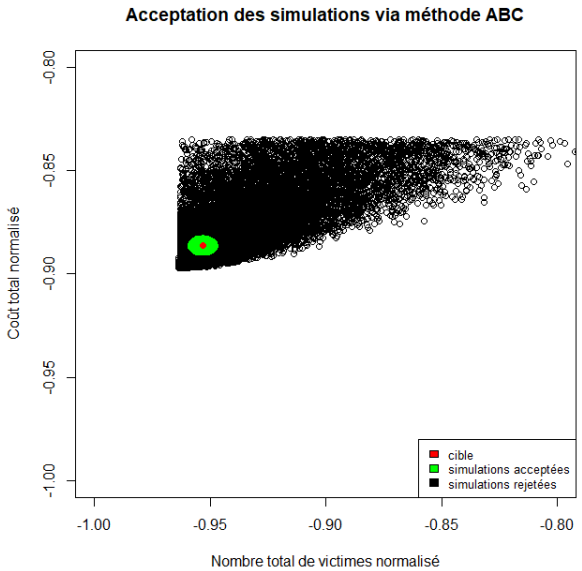


Figure 34 - Zone d'acceptation de la méthode ABC

- **Taux de transmission**

Traçons l'histogramme des taux de transmission de l'échantillon accepté :

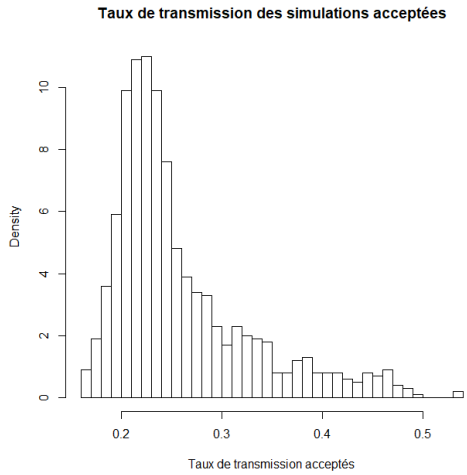
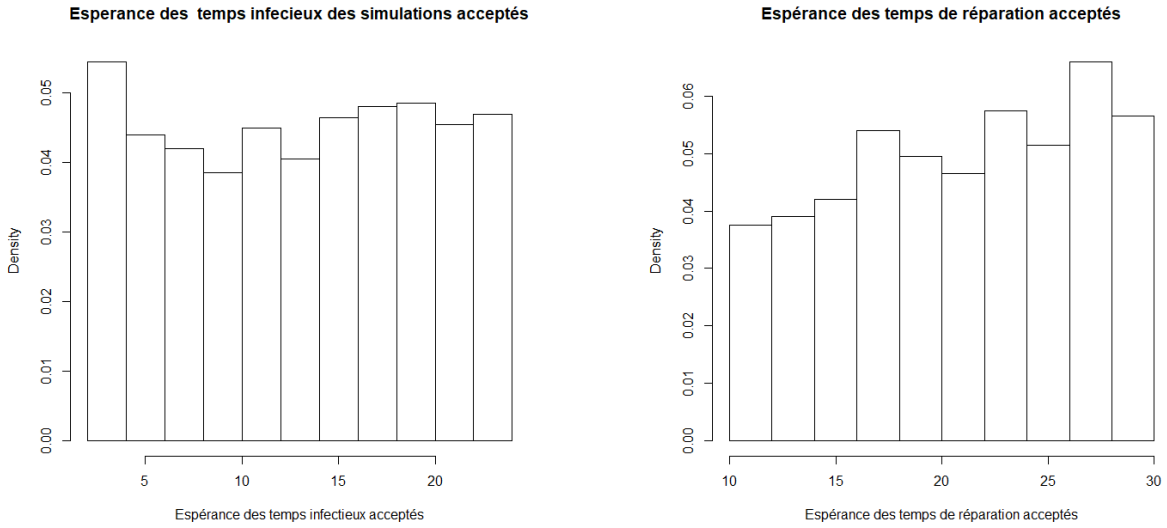


Figure 35 - Taux de transmission des simulations acceptées

La moyenne est de 0.26 sur l'échantillon accepté, ce qui est proche de la valeur trouvée lors pour le premier modèle. Cependant, l'asymétrie de l'échantillon accepté s'est bien inversée : la queue à gauche est bien plus fine que la queue à droite. Nous ne parvenons pas à ajuster une loi paramétrique sur ces données. Il faudra donc utiliser des méthodes non paramétriques à noyaux pour ajuster une densité à cet histogramme.
La queue de distribution est plus étendue et plus épaisse : les valeurs prises par α vont jusqu'à 0.5 contre 0.35 précédemment. Lors de notre premier estimation, seul α permettait de faire varier la taille de l'attaque d'une simulation à l'autre. Ici, le temps moyen infectieux peut lui aussi varier d'une attaque à l'autre et ainsi influencer le nombre de victimes. Ainsi, nous pensons que les variations des temps infectieux moyens permettent à α de prendre une amplitude de valeurs plus grande. Une anti-corrélation entre ces deux paramètres engendre un nombre de victimes stable. Intéressons-nous maintenant au temps infectieux de l'échantillon accepté pour confirmer ce phénomène.

- **Temps infectieux et de réparation**

Nous traçons l'histogramme des temps moyens infectieux et de réparation des simulations acceptées :



Pour les temps infectieux, notre première conjecture faite sur les 10 000 premières simulations (à savoir que les poids des faibles temps infectieux commençaient à prendre plus d'importance) n'est pas confirmée ici. En revanche, pour les temps de réparation acceptés, la tendance que nous avions décrite

sur les 10 000 premières simulations s'est confirmé : la distribution se concentre peu à peu sur la partie supérieure de l'intervalle donné *a priori*.

- **Corrélations des variables du modèle**

Afin de vérifier la présence d'une anti-corrélation entre les temps infectieux et le taux de transmission du virus nous calculons la matrice de corrélation de l'échantillon accepté. Le tableau suivant nous permet de regarder l'évolution des corrélations entre le passage de l'échantillon tronqué à l'échantillon accepté.

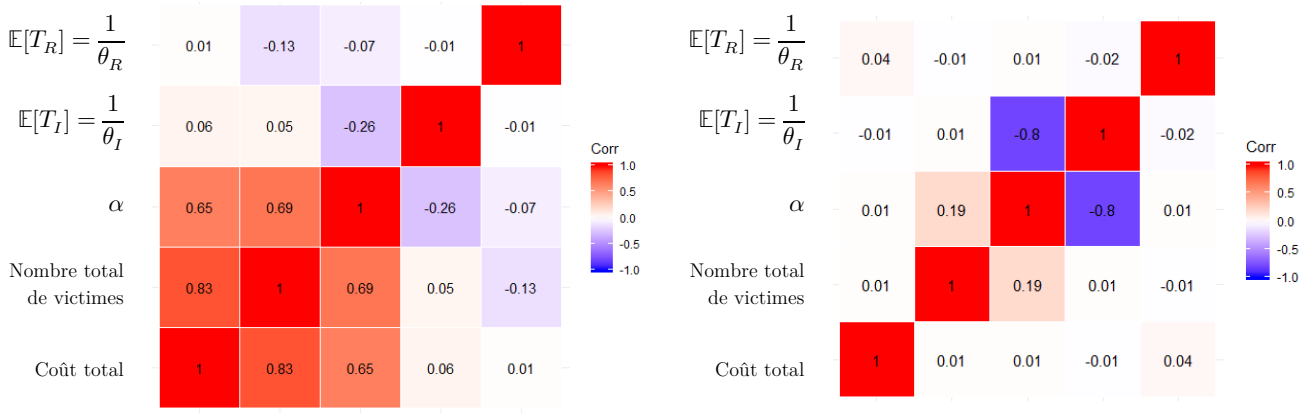


Figure 36-Matrices de corrélation sur les 37 972 simulations stockées (gauche) et sur les 1 000 simulations acceptées (droite)

Sur l'échantillon tronqué, on observe déjà une faible anti-corrélation (-0.26) entre la moyenne des temps infectieux et le taux de transmission : en ne stockant que les simulations générant une perte inférieure à 5 milliards d'euros on centre déjà notre attention sur la moitié des simulations dont le coût, et donc le nombre d'infectés est faible. On remarque que le coût total et le nombre total de victimes ne sont plus corrélés qu'à 0.65 et 0.69 avec le taux de transmission, contre 0.92 et 0.93 lors de la première approche d'estimation. L'introduction de nouveaux paramètres aléatoires relatifs aux temps infectieux et de réparation provoque cette baisse de corrélation en introduisant une variabilité supplémentaire.

En ce qui concerne l'échantillon accepté, avant de regarder la matrice de corrélation il faut avoir à l'esprit que le coût total et le nombre total de victimes sont quasi constants sur cet échantillon. Ayant pondéré notre métrique distance par 0.7 en faveur du coût total et 0.3 pour le nombre total de vicitmes, nous avons donc une variance qui est encore plus faible pour le coût que pour le nombre de vicitmes. Voici pourquoi sur l'échantillon accepté, on observe une corrélation quasi nulle du coût avec les autres variables du modèle. Le nombre de victimes varie lui un peu plus que le coût et présente tout de même une corrélation de 0.19 avec le taux de transmission α, ce qui est non négligeable mais tout de même faible par rapport à cette corrélation sur l'échantillon tronqué (0.69).
On observe une forte anti-corrélation entre le temps infectieux moyen et le taux de transmission (-0.8). Cette anti-corrélation explique la grande amplitude de valeurs possibles prises par ces deux variables, dont l'effet sur le nombre de victimes et donc sur le coût est de même signe. Si on regarde de plus près les valeurs de temps moyen prises lorsque le taux de transmission est supérieur à 0.4 on observe que toutes les valeurs moyenne des temps infectieux sont inférieures à 5. A l'inverse, lorsque le taux de transmission est inférieur à 0.2, les moyennes des temps infectieux se concentrent autour de 20.

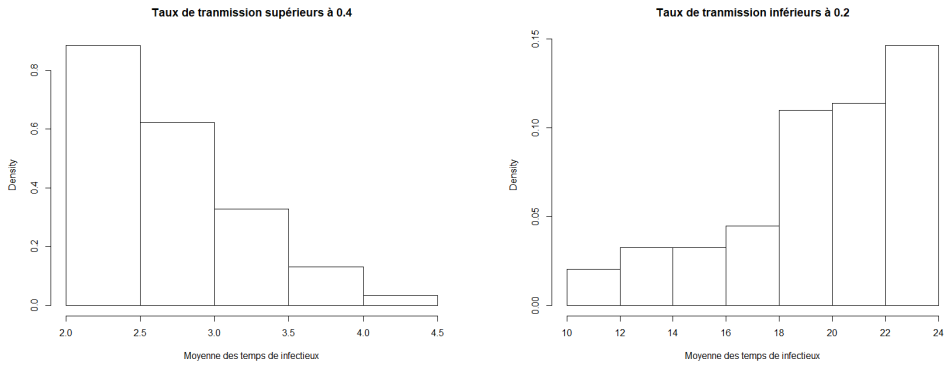


Figure 37 - Distribution des moyennes des temps infectieux selon les valeurs du taux de transmission

Si nous conservons ce modèle, nous devrons donc estimer la structure de dépendance entre le taux de transmission et le temps infectieux. Traçons la copule empirique obtenue avec les rangs normés pour avoir une idée de cette relation de dépendance :

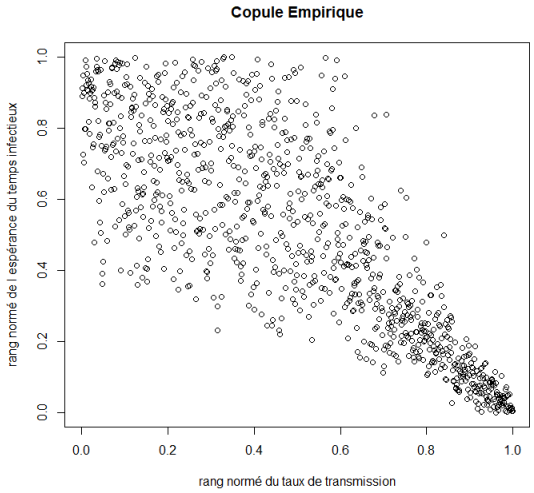


Figure 38 - Copule empirique liant le taux de transmission et l'espérance du temps infectieux

On observe bien une fonction décroissante témoignant de l'anti-monotonie entre nos deux variables. Lorsque le taux de transmission est faible, les valeurs prises par l'espérance du temps infectieux sont assez dispersées. Au contraire, lorsque le taux de transmission est élevé, les points sont très regroupés, ce qui témoigne d'une dépendance très forte.

- **Nombre total de victimes et coût total**

Comme précédemment, nous représentons le coût total et le nombre de victimes dans l'échantillon accepté.

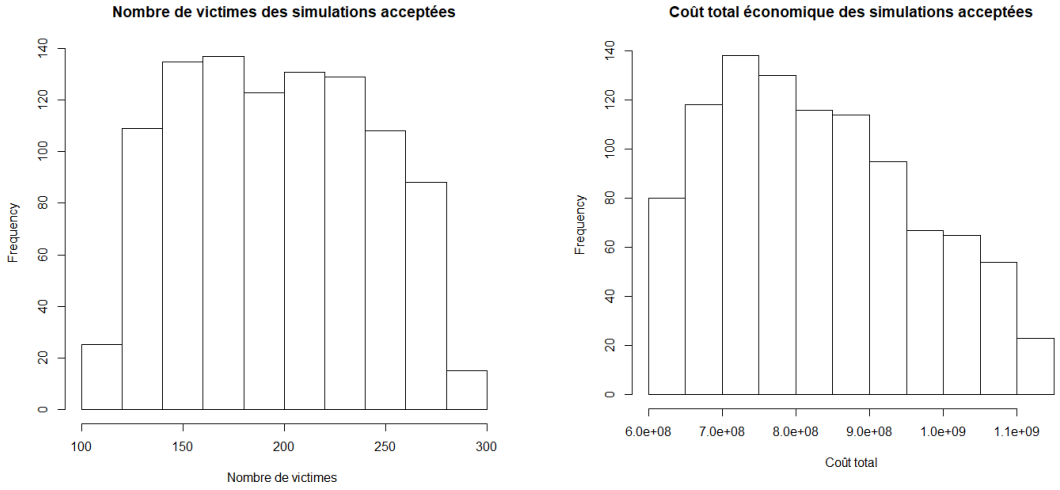


Figure 39 - Histogrammes du nombre de victimes et du coût total de l'échantillon accepté

On confirme ici que nos 1 000 simulations sélectionnées sont plus concentrées autours de la cible. Le coût moyen est de 829 millions d'euros contre 803 millions lors de la première approche. La fenêtre d'acceptation est aussi plus petite avec un coût maximum de 1.15 milliards et minimum de 600 millions d'euros. Le nombre moyen de victimes vaut 196 et est toujours proche de 200.La aussi la fenêtre d'acceptation est réduite puisqu'on accepte entre 111 et 290 victimes contre 61 et 337 précédemment.

- **Coût par police**

Intéressons-nous maintenant au coût par police :

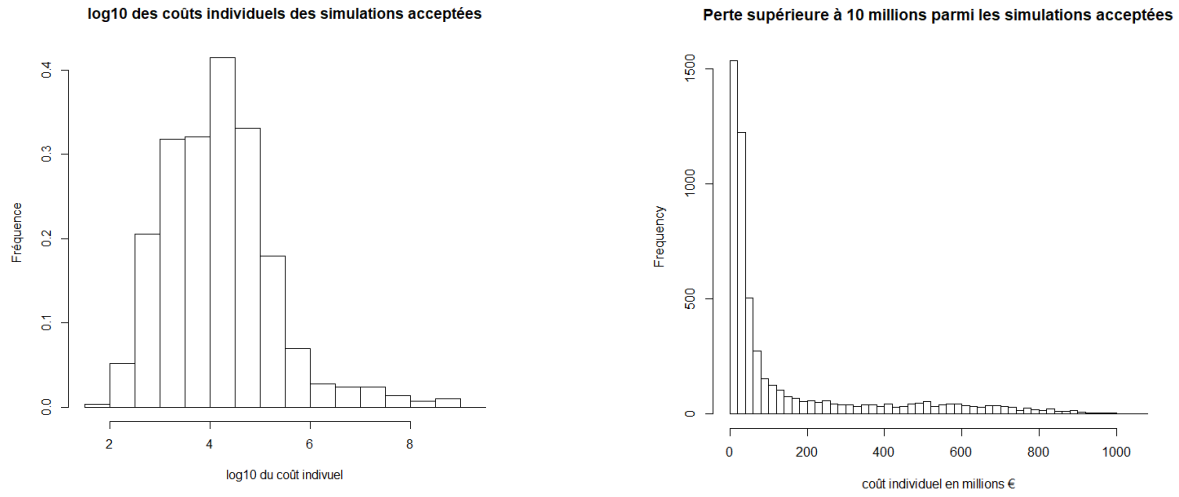


Figure 40 - Histogrammes des coûts individuels

Le coût médian est de 13 000 euros tandis que la moyenne est de 4.2 millions d'euros. Cet écart de résulte de valeurs très élevées prises par h sur certaines polices. Les grands coûts simulés par h ont un poids légèrement plus important que pour le premier modèle : nous avons toujours 5% des coûts au-dessus de 1 million mais maintenant 0.8% (au lieu de 0.7%) au-dessus de 100 millions et 0.5% (au lieu de 0.45%) au-dessus de 300 millions d'euros.

Par rapport au premier modèle on génère des coûts individuels légèrement plus sévères, ce qui est cohérent puisqu'on a un coût en moyenne plus élevé (829 millions contre 803 précédemment) réparti sur en moyenne moins de victimes (196 contre 204 précédemment).

Conclusion : Par rapport au premier modèle, cette approche génère des évènements dont le coût et le nombre de victimes sont plus proches de NotPetya. En regardant les 10 000 premières simulations nous avions en effet constaté que la valeur du quantile des distances d'ordre 2.5% était plus faible pour cette seconde approche que pour la première approche. L'analyse de l'échantillon accepté sur 100 000 simulations conforte aussi ce postulat. Au moment de sélectionner le modèle, il faudra prendre en compte que ce gain de précision vient avec une complexité supplémentaire de gestion des paramètres.

3.3.5 Troisième modèle

Nous allons proposer ici un troisième et dernier modèle dont nous estimerons les lois *a posteriori* des paramètres. Comme évoqué dans la première partie du mémoire, une approche par scénario permet à l'assureur d'évaluer le comportement de son portefeuille en cas de catastrophe. Il est donc intéressant de disposer de scénarios divers pour étudier leurs conséquences sur notre portefeuille.
Nous avons précédemment déterminé les paramètres permettant de reproduire des évènements proches de NotPetya. Mais qu'en est-il d'un évènement semblable à WannaCry ? WannaCry a touché 50 fois plus de victimes que NotPetya mais causé légèrement moins de pertes économiques : 8 milliards de dollars de perte économique totale contre 10 pour NotPetya (WannaCry a touché environ 100 000 entreprises contre 2 000 pour NotPetya). Ces deux virus ciblaient les systèmes opérant sur Windows, mais WannaCry a été bien moins destructeur que NotPetya. WannaCry était un ransomware qui encryptait les données des victimes afin de demander une rançon. NotPetya était une variante plus destructrice de type *wiper*, créée pour détruire les systèmes et les données s'y trouvant. [44] On peut donc se demander comment réagirait notre portefeuille dans le cas d'une attaque plus étendue mais moins sévère au niveau individuel.
Ce troisième et dernier modèle va nous permettre d'estimer la loi *a posteriori* des paramètres à l'origine de ces deux types d'évènements. Nous regarderons donc les simulations sur deux boules différentes centrées respectivement en NotPetya et WannaCry.

Nous avons vu lors de l'étude du premier modèle que WannaCry n'était pas atteinte par les simulations. Le coût associé à 10 000 victimes était nettement supérieur au coût de WannaCry. Il faudra donc travailler sur le paramètre de sévérité μ pour rendre possible une adéquation des paramètres aux deux attaques. Il faudra aussi analyser les corrélations entre les paramètres.

Nous anticipons une anti-corrélation entre d'un côté le taux de transmission et le temps infectieux influant sur le nombre de victimes et de l'autre côté les paramètres influant sur le coût par police tels que les temps de réparation et de sévérité. Cette anti-corrélation permettra d'ajuster le coût par assuré et le nombre de victimes afin d'atteindre les deux cibles.

3.3.5.1 Hypothèses du modèle

Comme nous l'avons évoqué lors de l'estimation, un point dont la perte totale s'élève à 8 milliards de dollars et faisant 50 fois plus de victimes que NotPetya ne peut être atteint par le modèle. Pour

atteindre ce point, le modèle doit être en mesure de générer des pertes par police plus faibles. Pour atteindre cet objectif, nous allons rajouter un aléa supplémentaire sur la borne supérieure du paramètre de sévérité et baisser sa borne inférieure à 0.01. La borne supérieure de la sévérité suivra une loi uniforme entre 0.02 et 0.9. Nous allons aussi diminuer la borne inférieure de l'intervalle des temps moyens de réparation. Nous avons donc les paramètres suivants :

Paramètre	Loi *a priori*
α	$U(0,1)$
θ_I	$\frac{1}{\theta_I} \sim U(2,24)$
θ_R	$\frac{1}{\theta_R} \sim U(1,30)$
θ_μ	$U(0.02,0.9)$

Tableau 40- Lois a priori des paramètres pour le troisième modèle

Pour ce troisième modèle les composantes de θ sont indépendantes et on a les lois marginales *a priori* suivantes : $\theta = \left(\alpha \sim U[0,1],\ \theta_I \sim l(2,24)\ ,\ \theta_R \sim l(1,30),\ \theta_\mu \sim U(0.02,0.9) \right)$

Nous avons effectué 500 000 simulations du scénario ransomware en utilisant les paramètres précédents et pour des questions de gestion de la mémoire avons stocké uniquement les simulations dont le coût total était inférieur à 2 milliards et le nombre de victimes inférieur à 20 000. Il nous reste 203 657 simulations stockées.

3.3.5.2 Validation de la méthode

Il est trop couteux de tester la validité du modèle sur l'ensemble des 203 657 points stockés. Nous avons tiré aléatoirement 10 000 points et appliqué la même méthode de validation que précédemment en prenant la grille d'ordres de quantiles suivante : 0.001, 0.01, 0.05, 0.1, 0.2, 0.4, 1, 2 et 4 pourcents. Les ordres des quantiles sont ici déterminés par rapport à l'échantillon stocké. Pour obtenir l'ordre d'un quantile par rapport à l'échantillon total, il suffit de multiplier ce dernier par (203 657)/(500 000). Notons que le test a plus de chances d'échouer proches de la frontière de troncature. Nous obtenons tout de même des scores de validation de 9.76, 70.82, 93.31, 96.26 98.10, 99.06, 99.74, 99.86 et 99.94 pourcents respectivement. Traçons le score de validité en fonction de l'ordre du quantile :

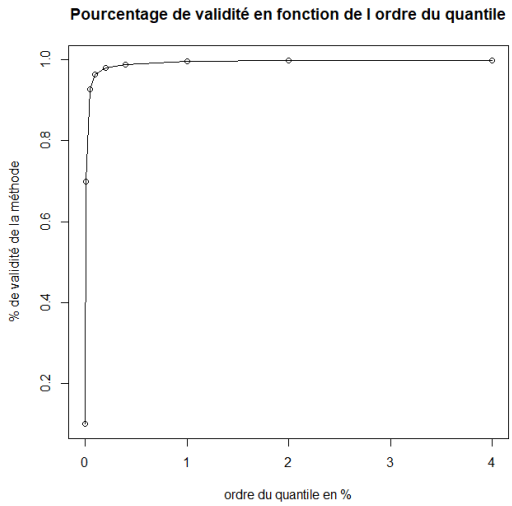


Figure 41 - Pourcentage de validité de la méthode en fonction de l'ordre du quantile

En utilisant toujours le même critère que pour les approches 1 et 2, on choisit un quantile optimal d'ordre 0.1% sur nos 203 657 simulations stockées, ce qui correspond environ à un quantile d'ordre 0.04% de nos 500 000 simulations totales.

3.3.5.3 Échantillon accepté autours des deux cibles

Regardons ce qu'il se passe lorsque nous acceptons les simulations autours des deux cibles. Pour le même ordre de quantile, on observe deux boules de tailles différentes. Le rayon de la boule centrée en NotPetya étant plus faible, on a donc des simulations plus concentrées autours de NotPetya que de WannaCry.

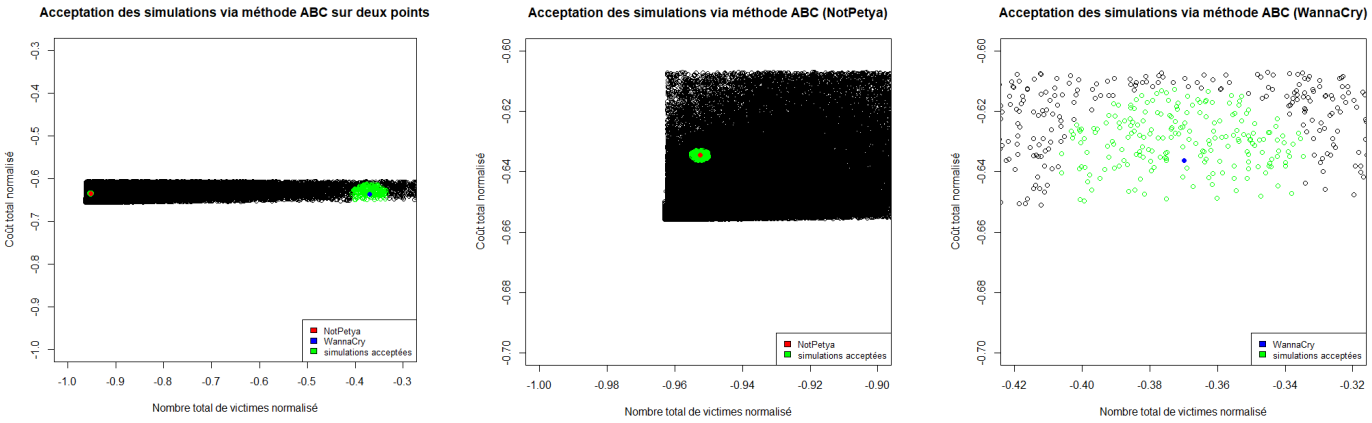


Figure 42- Graphiques des deux zones d'acceptations et zoom sur chacune des zones

Regardons maintenant le taux de transmission sur l'ensemble des deux boules. La moyenne empirique du taux de transmission sur l'échantillon accepté est de 0.40. L'histogramme suivant montre que la loi marginale du taux de transmission sur l'ensemble des deux boules est bimodale. En distinguant les simulations acceptées selon leur boule d'origine on constate que chaque mode correspond à une boule et que l'intersection de valeurs prises par le taux de transmission sur ces deux boules est quasi vide.

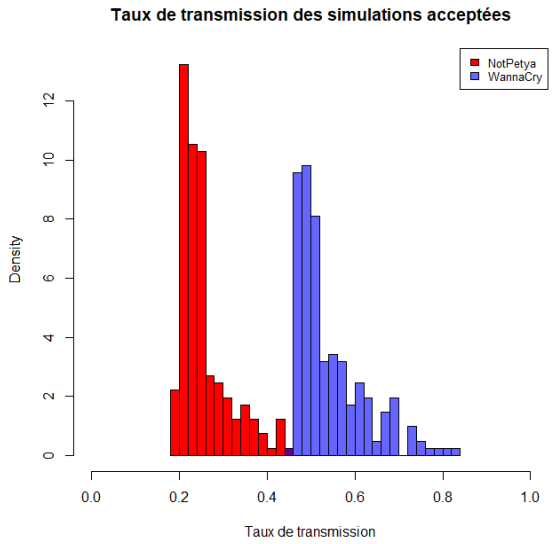


Figure 43 -Taux de transmission accepté selon l'attaque

Les taux de transmission correspondant à WannaCry sont plus élevés que ceux de NotPetya, ce qui est cohérent puisque le nombre de victimes est croissant du taux de transmission.
Cet histogramme laisse présager que la loi *a posteriori* des paramètres est différente sur chacune de ces boules.

Regardons les valeurs des paramètres sur chacune des boules d'acceptation (Tableau 41)

Nous ne parvenons pas à établir une tendance claire pour les espérances des temps infectieux des simulations acceptées. Comme pour la seconde approche, nous pensons que ce paramètre est anti-corrélé à α et permet d'équilibrer le nombre de victimes.
L'espérance du temps de réparation est clairement différente selon l'attaque approchée. Pour NotPetya les valeurs acceptées se sont concentrées sur la partie supérieure de l'intervalle avec un MAP à environ 28, tandis que pour WannaCry les valeurs acceptées sont presque toutes inférieures à 15, avec un MAP à environ 3.
La borne supérieure de la sévérité a elle aussi pris deux allures différentes selon l'attaque approchée : pour NotPetya elle s'est concentrée sur la partie supérieure avec un MAP autour de 0.8 tandis que pour WannaCry aucune valeur n'est supérieure à 0.30 et le MAP est inférieur à 0.05.

Nos paramètres influant sur le coût par police ont évolué de manière opposée sur chacune des deux boules, traduisant un fort impact par police pour NotPetya et un plus modéré pour WannaCry.

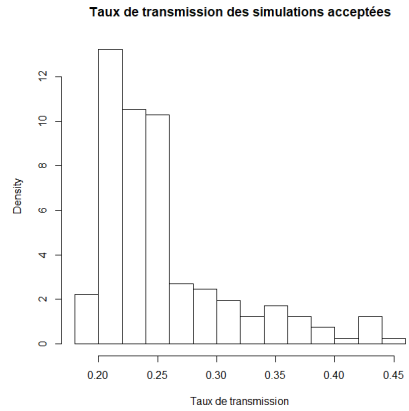
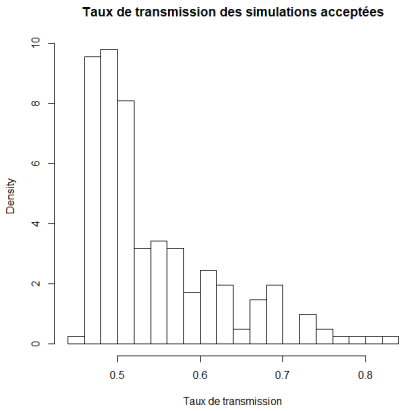
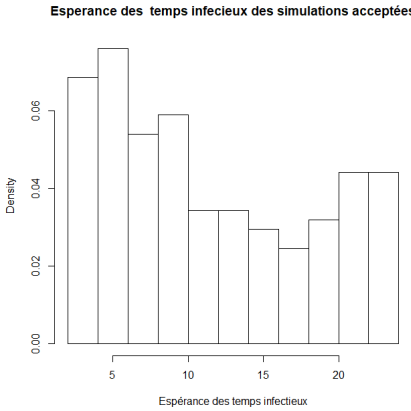
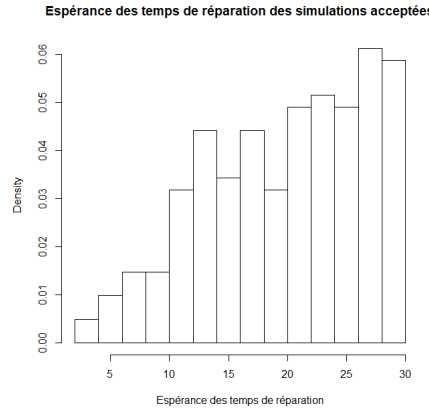
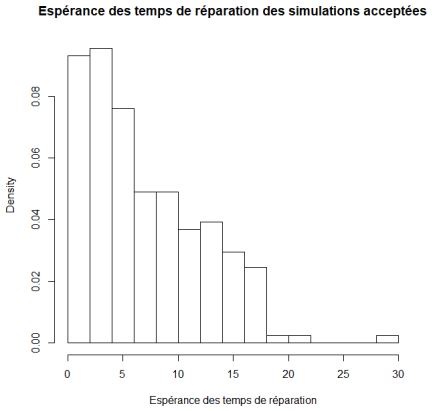
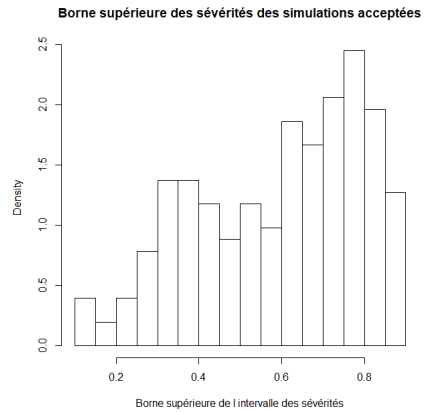
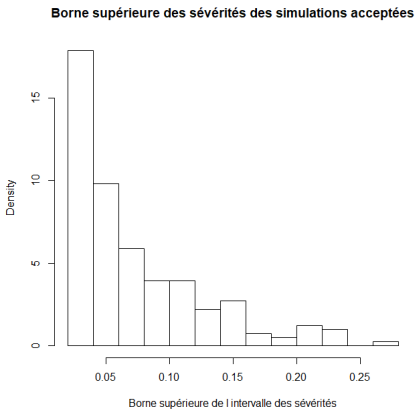
Paramètre	Boule autour de Notpetya	Boule autour de WannaCry
Taux de transmission α		
Espérance du temps infectieux		
Espérance du temps de réparation		
Borne supérieure de la sévérité		

Tableau 41-Comparaison des paramètres acceptés

- **Nombre de victimes et coût total**

Autour de NotPetya, le nombre moyen de victime est de 201 avec une fenêtre d'acceptation entre 156 et 242. Le coût total moyen est de 871 millions de dollars avec une fenêtre d'acceptation entre 944 millions et 803 millions d'euros. On est donc en moyenne plus proche de NotPetya que pour les 2 approches précédentes. Il est difficile d'attribuer la part de ce gain de précision à l'introduction d'un paramètre aléatoire supplémentaire puisque nous n'avons pas effectué le même nombre de simulations. Autour de WannaCry le nombre de victimes fluctue entre 9 344 et 10 604 et s'élève en moyenne à 9 981. Nous avons donc le nombre attendu de victimes. En revanche, pour le coût nous approchons moins bien la cible puisque nous avons un coût moyen de 1 milliard d'euros et une fenêtre comprise entre 1.7 milliards et 254 millions. Il faudrait réduire le rayon de la boule autour de WannaCry pour s'éviter une si forte amplitude.

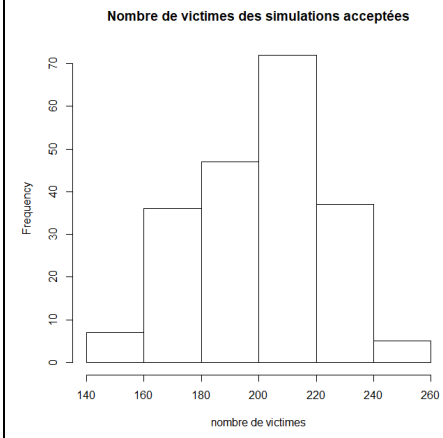
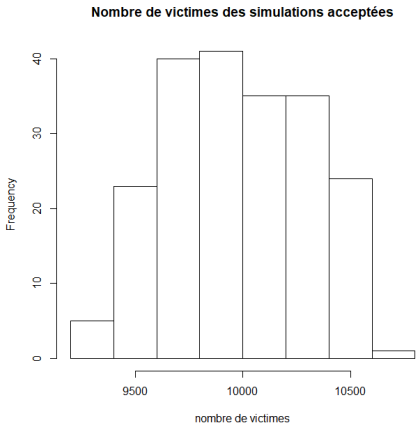
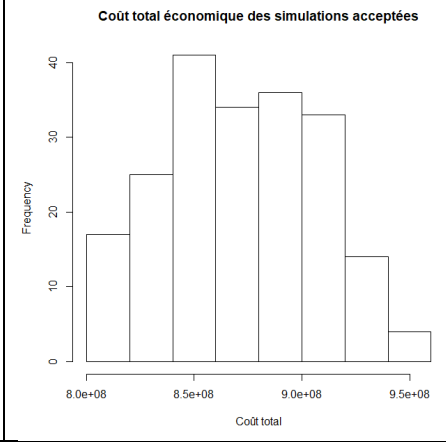
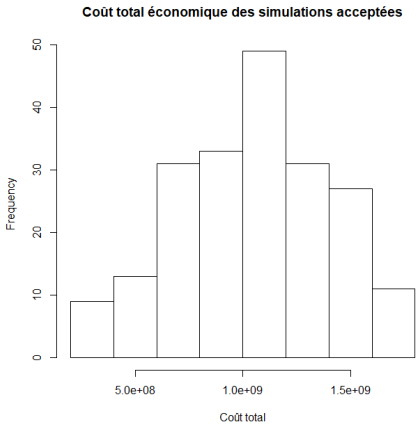
Variable	Boule autours de Notpetya	Boule autours de WannaCry
Nombre de victimes		
Coût total		

Tableau 42 - Comparaison du nombre de victimes et du coût total sur chaque boule

- **Coût par police**

Intéressons-nous maintenant au coût par police. Pour NotPetya, le coût médian est de 6 341 et la moyenne est de 4.3 millions d'euros. Le coût maximum est de 906 millions d'euros. Par rapport au second modèle, le coût moyen par police a augmenté et tandis que le coût médian a diminué. Cela indique que nous simulons davantage de très grands coûts. Nous avons désormais 4.35% (contre 5% pour la seconde approche) des coûts supérieurs à 1 million d'euros, 0.73% des coûts supérieurs à 100 millions (contre 0.8% pour la seconde approche) et 0.54% des coûts supérieurs à 300 millions d'euros (contre 0.5% pour la seconde approche) .

Pour WannaCry, nous avons un coût médian de 400 euros et un coût moyen de 105 234 euros. Le coût maximum s'élève à 622 millions d'euros. Seulement 1.25% des coûts sont supérieurs à 1 million et 0.005% sont supérieurs à 100 millions.
Nous avons bien deux évènements totalement différents atteints par notre modèle.

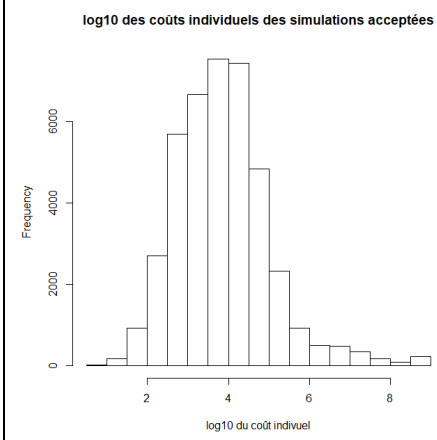
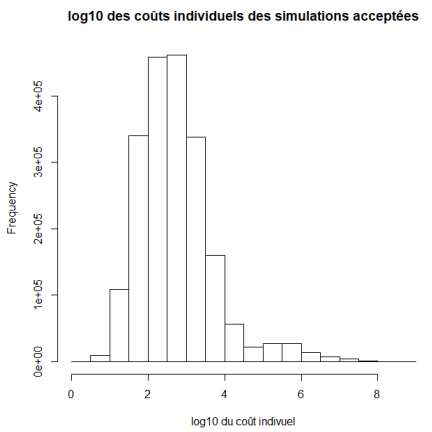
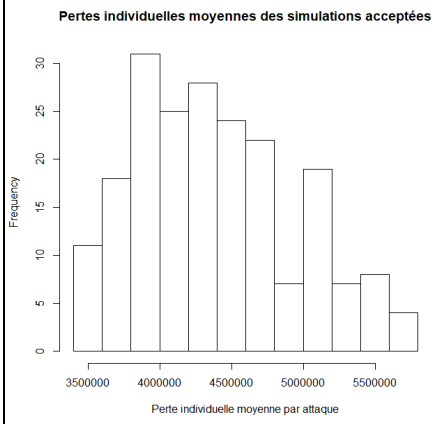
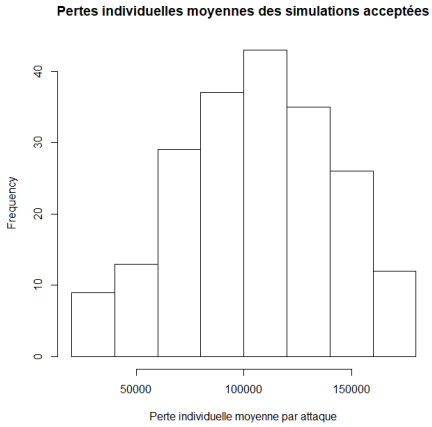
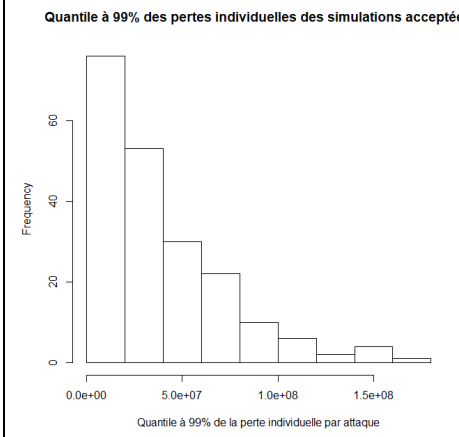
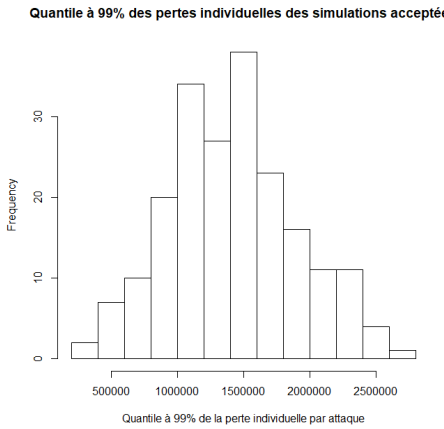
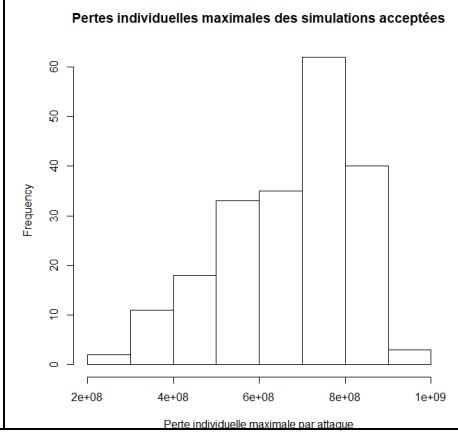
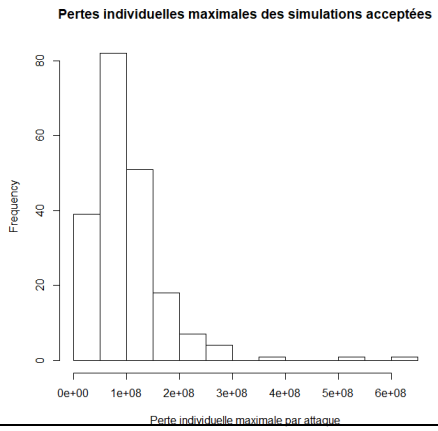
Variable	NotPetya	WannaCry
Coût par police (toutes simulations acceptées confondues)		
Perte Moyenne (par simulation acceptée)		
Quantile à 99% de la perte (par simulation acceptée)		
Perte Maximale (par simulation acceptée)		

Tableau 43 - Caractéristiques du coût par police autour de NotPetya et WannaCry

3.3.5.4 Échantillon accepté autours du segment reliant les deux cibles

Nous avons vu que la loi *a posteriori* était différente autour de chacune des deux cibles. Lorsqu'on regarde les lois marginales des paramètres sur les deux boules à la fois, on obtient par exemple une loi bimodale pour le taux de transmission. Cela signifie que les paramètres du modèle suivent des lois différentes selon la cible. Il existe donc une variable discrète à deux modalités conditionnant le comportement des paramètres sur les deux boules jointes.

Au lieu de regarder séparément les lois *a posteriori* sur chacune des deux boules et utiliser une variable latente à deux modalités pour conditionner l'utilisation de ces deux lois lors de futures simulations, nous choisissons d'accepter aussi les éléments au milieu de ces deux cibles. Cette démarche revient à supposer que des évènements se situant entre NotPetya et WannaCry en termes de nombre de victimes et de coût par police sont susceptibles de se produire.
Pour accepter les simulations, nous déplaçons le centre de la boule d'acceptation avec un pas régulier sur le segment reliant nos deux points. A chaque fois que la boule change de centre, nous acceptons des points supplémentaires. Nous choisissons d'abaisser l'ordre du quantile à 0.05% au lieu de 0.1% afin d'éviter une trop grande amplitude de coût prise au voisinage de WannaCry (le coût total moyen sur les deux boules s'élevait à 960 millions d'euros). Comme nous l'avions vu, ce choix de quantile fournit un score élevé de validité de 92.7%. Nous obtenons la zone d'acceptation suivante :

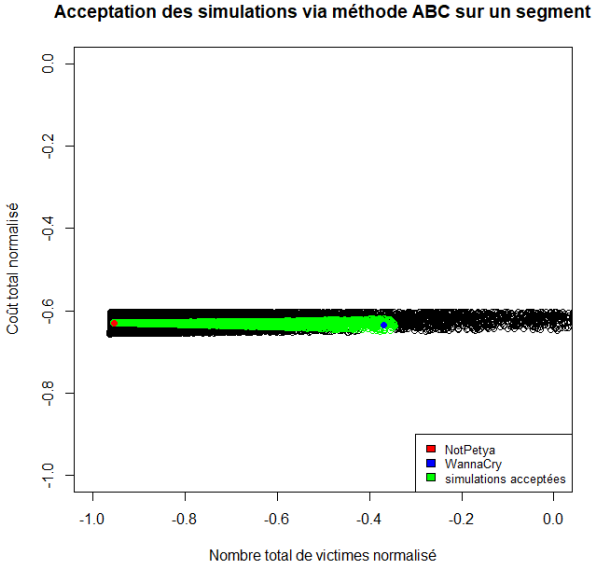


Figure 44 - Zone d'acceptation autour du segment reliant NotPetya et WannaCry

En regardant de plus près, on constate que la concentration de points simulés est plus élevée proche de NotPetya que de WannaCry. Ainsi, l'échantillon accepté en déplaçant le centre de la boule d'acceptation avec un pas régulier accorde plus de poids aux évènements proches de NotPetya qu'aux évènements proches de WannaCry. Si on simulait en suivant la loi de l'échantillon ainsi accepté, on tomberait plus souvent sur des évènements proches de NotPetya que de WannaCry. Or, nous voudrions simuler des évènements répartis uniformément sur le segment que nous avons tracé. Sur le graphique suivant à gauche on remarque bien que le nombre de victimes n'est pas réparti uniformément entre 200 et 10 000 comme nous le souhaitons, mais qu'il est plus concentré sur les faibles valeurs, ce qui atteste d'un plus grand nombre de points acceptés autours de NotPetya que de WannaCry.

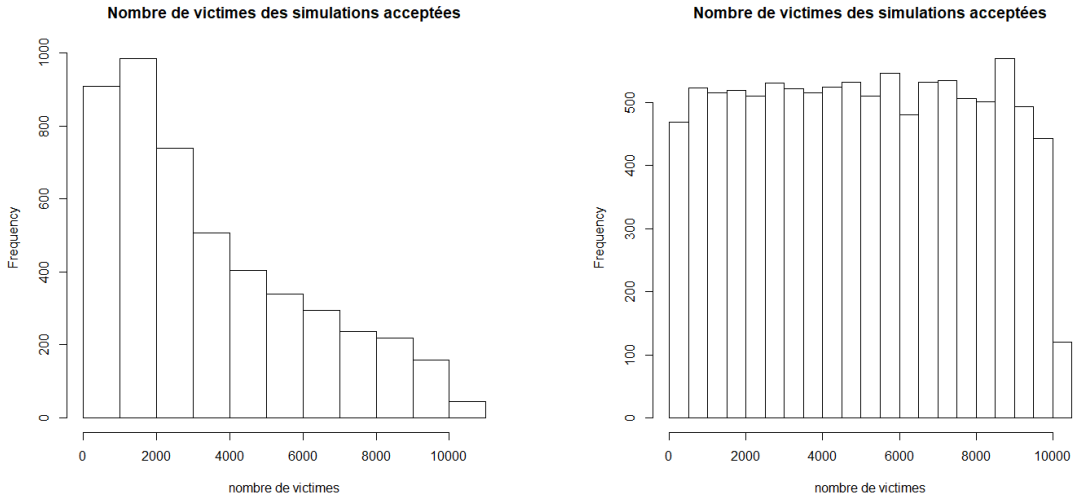


Figure 45 - Nombre de victimes des simulations acceptées selon la méthode d'acceptation : sans répétition (gauche), avec répétition (droite)

Ce phénomène s'explique de la manière suivante. Lorsque nous déplaçons la boule d'acceptation avec un pas régulier, puisque les rayons des boules proches de NotPetya sont plus faibles que ceux proches de WannaCry, le cardinal de l'intersection entre deux boules successives proches de NotPetya est plus petit que celui entre deux boules successives proches de WannaCry. Ainsi, l'ensemble des points uniques acceptés par deux boules successives est plus grand pour NotPetya que pour WannaCry.
Deux options s'offrent à nous pour équilibrer l'importance de nos évènements dans l'échantillon accepté : faire varier le pas de déplacement sur le segment ou accepter avec répétition les points situés dans l'intersection de deux boules. Nous choisissons la seconde proposition qui est plus commode.
Lorsque nous acceptons avec répétition, nous obtenons la répartition présentée dans le graphique de droite : on constate bien une répartition uniforme du nombre de victimes comme souhaité. Ainsi, nous accordons le même poids à chaque type d'évènement.

Nous obtenons 10 404 vecteurs de paramètres acceptés.
Regardons les simulations acceptées.

-Taux de transmission α

Traçons l'histogramme du taux de transmission des simulations acceptées autours de notre segment :

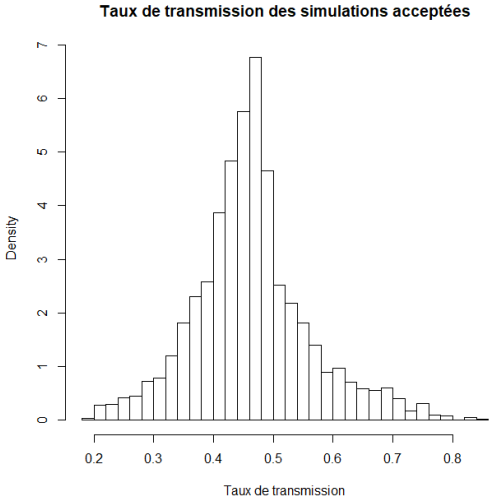


Figure 46 - Taux de transmission acceptés sur le segment

Nous avons désormais une loi uni-modale, dont la moyenne est 0.46, ce qui est nettement supérieur aux deux premières approches. Nous aurons donc en moyenne plus de victimes avec cette approche qu'avec les deux précédentes. Le skewness vaut 0.50 ce qui indique une queue de distribution plus fine à gauche qu'à droite.

- **Temps infectieux, temps de réparation et sévérité**

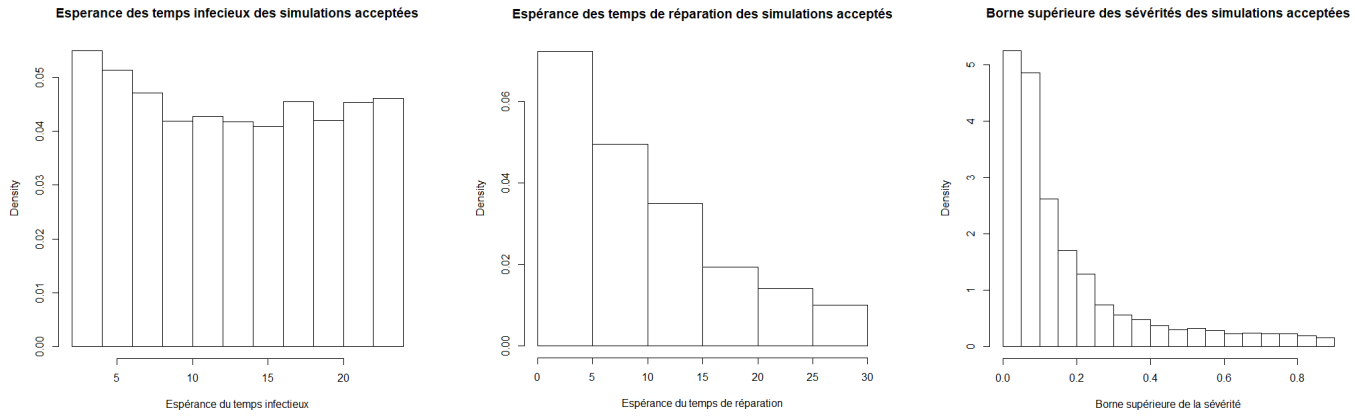


Figure 47 - Distribution des paramètres acceptés sur le segment

Nous n'observons pas de tendance particulière pour les espérances des temps infectieux acceptés. Cette variable permet de contre balancer la valeur du taux de transmission et influe légèrement sur la perte BI. Les espérances des temps de réparation et les bornes supérieures des sévérités se sont concentrées principalement sur la moitié inférieure de leur ensemble de définition puisque dès que nous nous éloignons de NotPetya pour rejoindre WannaCry, les coûts par police diminuent pour rester proche du segment. Regardons de plus près le coût total et le coût par police.

- **Coût total et coût par police**

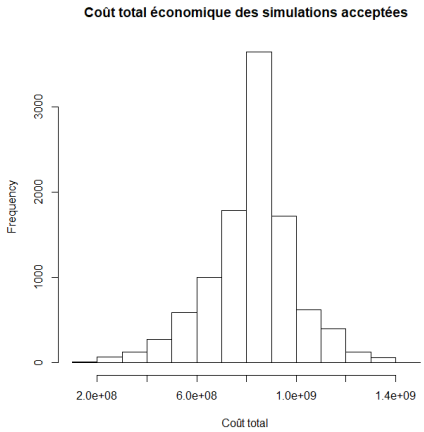


Figure 48 - Coût total des évènements acceptés

Coût total moyen de 824 millions d'euros qui se situe bien entre 874 millions (NotPetya) et 699 millions (WannaCry). Le coût est tout de même supérieur à la moyenne attendue de 786.5 millions. Même en ayant réduit la valeur du quantile, certaines simulations proches de NotPetya sont acceptées alors

qu'elles sont relativement éloignées. Le modèle parvient à atteindre WannaCry avec plus de difficulté que pour NotPetya, ce qui est logique puisque nous avons fait notre étude principalement sur NotPetya et avons construit la fonction de coût h uniquement en utilisant des informations sur les victimes de NotPetya. Un travail plus approfondi sur h est à envisager pour mieux atteindre WannaCry.

Concernant le coût individuel, nous avons un coût médian de 827 euros et une moyenne de 181 797 euros. Le coût maximum relatif à une police atteint 1.02 milliards. 1.62% des coûts individuels sont supérieurs à 1 million et 0.02% sont supérieurs à 100 millions.
On se situe en moyenne entre nos deux évènements.

- **Corrélations des variables du modèle**

Regardons les corrélations au sein de l'échantillon accepté.

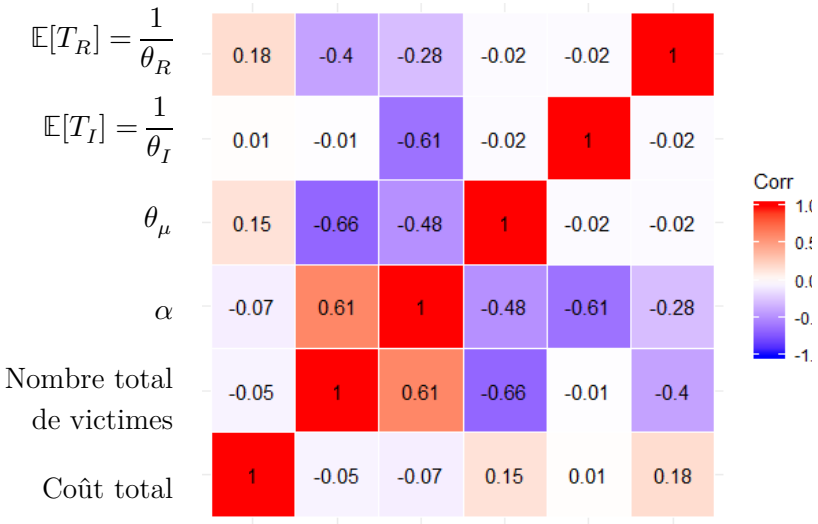


Figure 49 - Matrice de corrélation des paramètres acceptés sur le segment

Comme nous l'avions anticipé, nous avons une anti-corrélation entre d'un coté le taux de transmission influant sur le nombre de victimes et de l'autre coté θ_μ, la borne supérieure de μ (-0.48) et l'espérance du temps de réparation (-0.28) qui influent positivement sur le coût par police. L'espérance du temps infectieux est anti-corrélée au taux de transmission (-0.61) comme lors de la seconde approche d' estimation. Il y a donc encore un équilibre qui s'établit entre le taux de transmission et l'espérance du temps infectieux afin de générer le bon nombre de victimes.
Le coût total est quasi stable sur l'échantillon accepté, il est donc très peu corrélé aux autres variables. On note tout de même de faibles corrélations positives du coût total avec la borne supérieure de la sévérité (0.15) et l'espérance du temps de réparation (0.18), ce qui est tout à fait logique : plus la proportion d'ordinateurs touchés et le temps de réparation est important, plus le coût de l'évènement sera important.
Le nombre de victimes est lui corrélé négativement avec la borne de supérieure de la sévérité μ (-0.68) ainsi qu'avec l'espérance du temps de réparation (-0.4). Lorsque le coût par nombre de victimes diminue, le coût par police augmente et on se rapproche donc de NotPetya. A l'inverse, lorsque le nombre de victimes augmente, le coût par police diminue et l'évènement généré se rapproche alors de WannaCry.

Conclusion : NotPetya était un évènement de forte sévérité individuelle et de 'faible' étendue, tandis que WannaCry avait une sévérité individuelle moins importante mais une plus grande portée. En nous déplaçant entre NotPetya et WannaCry pour construire notre zone d'acceptation, nous prenons le parti qu'un évènement se situant entre ces deux attaques pourrait avoir lieu. Cette approche rend possible la simulation d'évènements de types différents, ce qui nous permettrait d'étudier quel genre d'évènement pénalise le plus notre portefeuille d'assurés.

3.3.6 Choix du modèle

Avant de simuler la perte assurée, choisissons le modèle à utiliser.
Le premier modèle présente l'avantage d'être facile à implémenter et assez proche de la cible initiale NotPetya.
Le second modèle n'apporte pas de possibilités supplémentaires et complexifie la gestion du modèle, nous l'écartons donc.
Le troisième modèle dont la loi *a posteriori* des paramètres est estimée autours du segment reliant NotPetya et WannaCry permet de simuler des évènements de natures diverses : des évènements de forte sévérité individuelle et de faible portée (NotPetya), des évènements de moins grande sévérité individuelle et de plus grande portée (WannaCry), ou bien des évènements centraux nouveaux mais vraisemblables puisqu'ils se situent entre NotPetya et WannaCry.
Nous sommes intéressés par la possibilité de simuler des évènements variés afin d'étudier le comportement du portefeuille suivant la nature de l'évènement et pensons que des évènements entre NotPetya et WannaCry sont susceptibles de se produire.
Nous choisissons donc le troisième modèle obtenu pour simuler la perte assurée.

3.4 Simulations de la perte assurée

Nous avons retenu le troisième modèle pour construire le scénario ransomware. Dans cette partie nous allons désormais nous intéresser à la perte assurée générée en utilisant ce troisième modèle.
Il faut distinguer la perte par évènement de la perte annuelle. Les pertes par évènement sont renseignées dans une *Event Loss Table* (ELT) tandis que les pertes par année sont renseignées dans une *Yearly Loss Table* (YLT). Une ELT traite les évènements de manière individuelle et retranscrit uniquement la sévérité des évènements tandis qu'une YLT associe les évènements de l'ELT entre eux en ajoutant la notion de fréquence d'évènements par année. Pour une même année, on peut très bien avoir zéro, un ou plusieurs évènements d'accumulation. Dans ce mémoire, nous ne présenterons que la distribution de la perte par évènement.

Dans l'intégralité de cette partie, les données utilisées pour simuler la perte assurée sont fondées sur des portefeuilles existants mais ont été significativement altérées. Cela concerne notamment les montant des limites de police, de couverture et la répartition des sous-garanties dans les contrats.

3.4.1 Méthode de simulation du vecteur de paramètres

Pour simuler notre scénario ransomware nous devons d'abord choisir comment obtenir le vecteur de paramètres du modèle. Plusieurs options s'offrent à nous :
- estimer les lois marginales de manière non paramétrique, puis ajuster une copule pour gérer les dépendances au sein des variables du vecteur de paramètres.
- entrainer un classifieur sur l'espace des paramètres. Ce classifieur prédirait 1 lorsque le vecteur de paramètres est accepté par ABC et 0 sinon.
- procéder par bootstrap sur l'échantillon accepté par ABC

La première méthode est la plus naturelle puisqu'elle permet d'obtenir la loi a posteriori $\pi(\theta|y)$. Une fois les lois marginales et la copule estimée il serait possible de simuler selon $\pi(\theta|y)$. Pour ne pas surcharger la gestion des paramètres du modèle, nous n'utiliserons pas cette méthode.
La seconde méthode permet d'obtenir un proxy de la méthode ABC utilisée précédemment. La possibilité de ne pas recourir aux simulations du SIR et au calcul des pertes serait un gain de temps considérable. Nous écartons cette méthode car sa fiabilité dépendra fortement de la qualité du classifieur.
La troisième méthode est celle que nous utiliserons afin de simplifier l'utilisation du modèle. Elle présente l'inconvénient de ne pas générer de nouveaux points par rapport à ceux acceptés. Dans notre cas nous avons un échantillon suffisamment grand pour compenser cet inconvénient. Nous stockons dans une table les vecteurs acceptés via la méthode ABC et tirons ensuite avec remise parmi les vecteurs de cette table pour simuler le scénario ransomware.

3.4.2 Simulations de la perte assurée

3.4.2.1 Hypothèses de simulations et objectifs

Pour effectuer nos simulations, nous rendons aléatoires les hyper-paramètres que nous avions fixés pour l'estimation et utilisons un bootstrap sur l'échantillon des θ acceptés en 3.3.5.4).

On s'affranchit donc des conditions fixées pour l'estimation, à savoir :
- la proportion d'assurés vulnérables au virus
- la durée maximum de l'attaque (modélisée par le temps avant l'arrivée d'un patch)
- le coût de la rançon.

La table donnant la proportion d'assurés vulnérables au virus a déjà été introduite lors de la présentation du scénario ransomware (section 3.2.5 Tableau 35).
Nous avions vu que les deux attaques, NotPetya et WannaCry, avaient été stoppées rapidement. Nous voulons donc étudier l'impact d'une attaque de plus grande durée. Pour chaque attaque, nous simulerons T_P selon une loi exponentielle de paramètre $\frac{1}{24}$. Ainsi nous avons aurons un temps moyen d'attaque de 24 heures et un écart-type de 24 heures permettant de simuler des attaques bien plus longues.
Les deux attaques étudiées avaient des rançons assez faibles comprises entre 300 et 600 dollars. Le coût de la rançon étant totalement déterminé par le hacker, il n'est pas impossible de voir le prix des rançons augmenter. Pour les simulations, la rançon pourra coûter 500, 1 000, 5 000 ou 10 000 dollars. On prend

donc : $P(X = 500) = P(X = 1\ 000) = P(X = 5\ 000) = P(X = 10\ 000) = \frac{1}{4}$ et on suppose que X est totalement indépendant des autres variables du modèle.

Attention, nous avons estimé la loi *a posteriori* de θ pour P, X et T_P fixés. L'estimation de la loi *a posteriori* de θ correspond donc en réalité à $\pi(\theta|y, P = 0.467, X = 600, T_P = 24)$. Utiliser cette même loi a posteriori pour simuler d'autres attaques avec des valeurs de P, X et T_P différentes revient à supposer l'indépendance entre θ et P, X et T_P.
Il est légitime de supposer cette indépendance si nous souhaitons répondre à la question suivante : « Qu'aurait-il pu se passer si les virus NotPetya, WannaCry ou un compromis entre les deux avaient visé un autre système d'exploitation, que le coût de la rançon avait été plus élevé et que l'attaque n'ait pas été endiguée si vite ? ».

Ce modèle ne permet pas de répliquer ni prévoir le comportement de n'importe quel type de ransomware sur notre portefeuille. En revanche, il permet de simuler des variantes proches de NotPetya ou WannaCry dans des conditions plus adverses, pouvant être qualifiées de scénarios catastrophe.

3.4.2.2 Étude des évènements générés par le modèle

Nous effectuons 50 000 simulations en procédant par bootstrap sur les paramètres de l'échantillon accepté et en simulant indépendamment la proportion d'assurés vulnérables, la durée maximum de l'attaque et le coût de la rançon.
Regardons tout d'abord le coût total et le nombre de victimes de nos évènements.

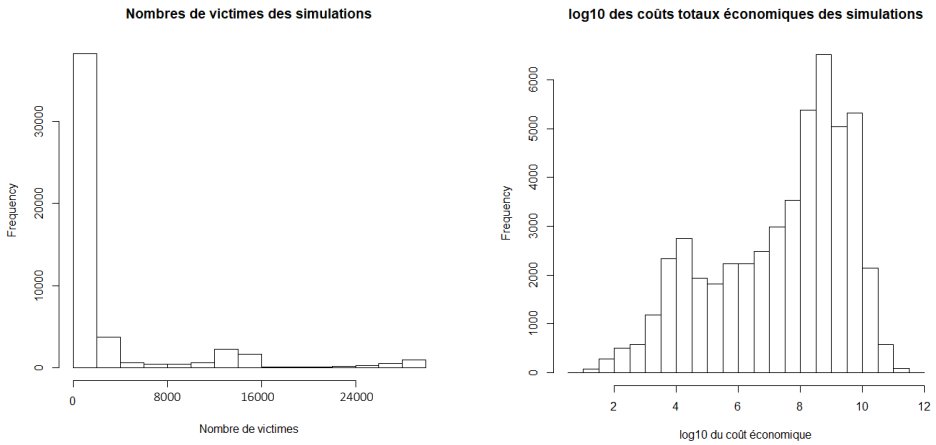


Figure 50 - Nombre de victimes et coût total des 50 000 évènements générés

En traçant l'histogramme du nombre de victimes, on observe des pics autours de certaines valeurs (inférieur à 4 000, 16 000, 30 000). Nous verrons que ces pics correspondent aux évènements provenant d'une même proportion d'entreprises vulnérables au virus, donc au même système d'exploitation attaqué.
Notons qu'un nouveau type d'évènement peut être généré par le modèle : une attaque de même sévérité par police que NotPetya, mais dont le nombre de victimes serait plus important. Ce nombre de victimes plus important peut être produit grâce à deux variables : le temps avant l'arrivée du patch et le système d'exploitation attaqué. Plus le temps avant l'arrivée du patch est long, plus le virus se propage. Une part importante de systèmes d'exploitation vulnérables pourra potentiellement engendrer un grand nombre de victimes si la durée de l'attaque est assez longue.

Concernant le coût total économique, on a une moyenne de 2.4 milliards d'euros et une médiane à 100 millions d'euros. Ce décalage indique la présence de très fortes valeurs. On a en effet des évènements allant de quelques centaines d'euros à 92 milliards d'euros.

Traçons le coût des évènements en fonction du nombre de victimes afin de mieux comprendre où se situent les évènements générés par rapport à NotPetya et WannaCry :

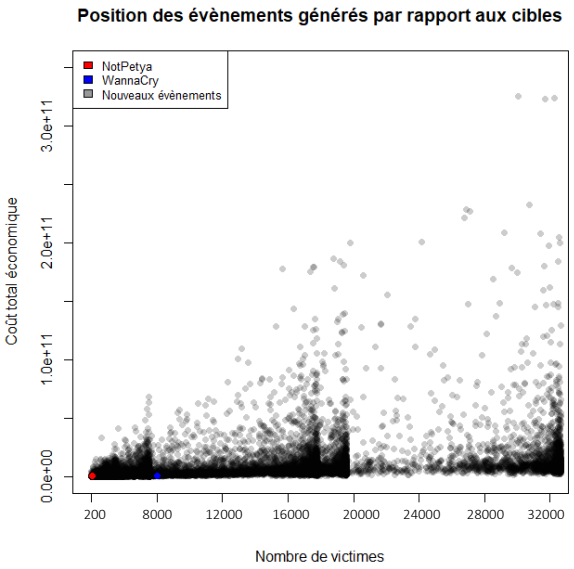


Figure 51 - Simulations par rapport à NotPetya et WannaCry

Le graphique donne l'impression que les simulations se sont fortement éloignées de nos deux cibles, ce qui permet d'atteindre des évènements de natures diverses. Cependant, si on met cette figure en relief avec nos deux histogrammes précédents, nous constatons que la plus grande masse des simulations est concentrée autour de NotPetya et WannaCry. On a en effet uniquement 16.15% de simulations qui dépassent 10 000 victimes et 27.85% des simulations dépassent 875 millions d'euros. Nous avons 16% des évènements qui dépassent NotPetya en coût et WannaCry en nombre.

Étudions l'impact des variables que nous avons rendues aléatoires.
Regardons d'abord l'influence de la proportion vulnérable sur nos simulations. Nous traçons de couleur différente les points selon la proportion vulnérable à l'origine de la simulation.

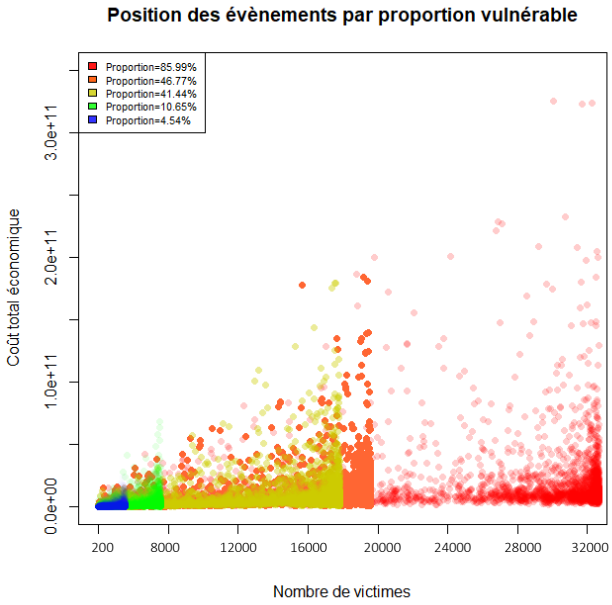
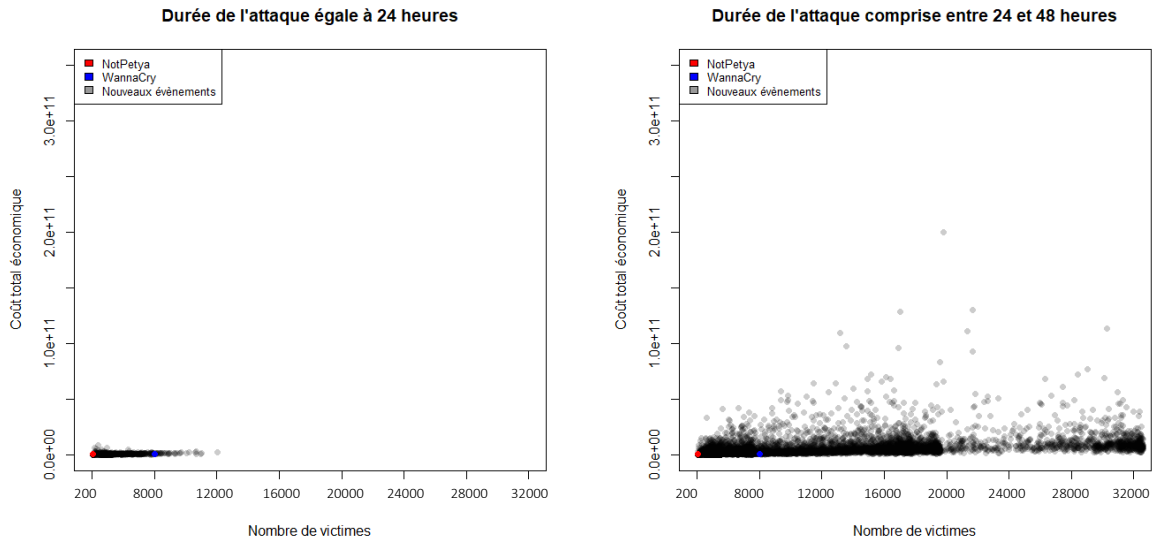


Figure 52 - Influence de la proportion vulnérable sur les simulations

Sur le graphique précédent, on voit bien que le nombre de victimes est majoré par le nombre total d'entreprises vulnérables. Lorsque le temps de l'attaque devient trop important, toutes les entreprises vulnérables peuvent être touchées. Quand le temps avant l'arrivée du patch est inférieur à 24 heures, quel que soit la proportion d'entreprises vulnérables au virus, le nombre maximum de victimes s'élève à 12 025 et le nombre de victimes moyen est 375. Regardons justement plus en détails nos simulations selon le temps nécessaire avant l'arrivée d'un patch.



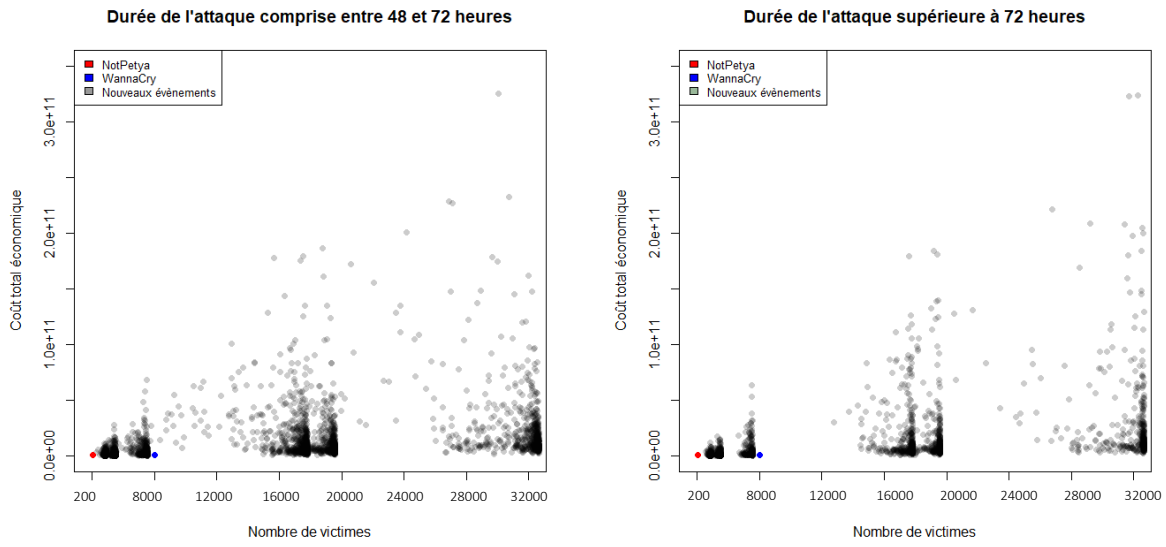


Figure 53 - Simulations selon le temps avant l'arrivée d'un patch

Pour les simulations issues d'un temps de patch égal à 24 heures, on retrouve des simulations proches de NotPetya et WannaCry. La proportion d'entreprises vulnérables prend 4 valeurs en dessous de celle utilisée pour l'estimation, et seulement une au-dessus. À temps de patch égal, il y a donc une plus forte concentration d'évènements entrainant un faible nombre de victimes. Les évènements dépassant WannaCry en nombre de victimes proviennent de la plus forte proportion de vulnérables.
Lorsque le temps d'attaque se situe entre 24 et 48 heures tous les nombres de victimes sont atteints, tandis que lorsque le temps de l'attaque devient trop important, le nombre de victimes se concentre proche du nombre d'entreprises initialement vulnérables au virus.
De manière plus générale, lorsque la durée de l'attaque est faible, les autres variables influant sur le nombre de victimes (comme le taux de transmission et la proportion d'entreprises vulnérables) n'ont pas le temps d'avoir un impact conséquent sur le nombre final de victimes : quel que soit la proportion vulnérable et le taux de transmission, si l'attaque est stoppée suffisamment vite, elle fera peu de victimes. En revanche, T_P suffisamment élevé permet de constater les effets des autres variables sur le nombre de victimes.

En procédant de la même manière que pour la figure 55 nous n'observons pas de tendance particulière insufflée par le coût de la rançon. Nous regarderons plus précisément l'impact du coût de la rançon au moment de calculer les corrélations.

Pour résumer, la proportion vulnérable fixe le nombre maximum de victimes tandis que l'augmentation de la durée de l'attaque associé à un taux de transmission et des temps infectieux suffisamment élevé permettent d'atteindre ce nombre.

3.4.2.3 Impacts sur la perte assurée

Regardons tout d'abord comment sont corrélés les paramètres du modèle avec la perte assurée et la perte économique et tentons de déduire des caractéristiques de notre portefeuille.

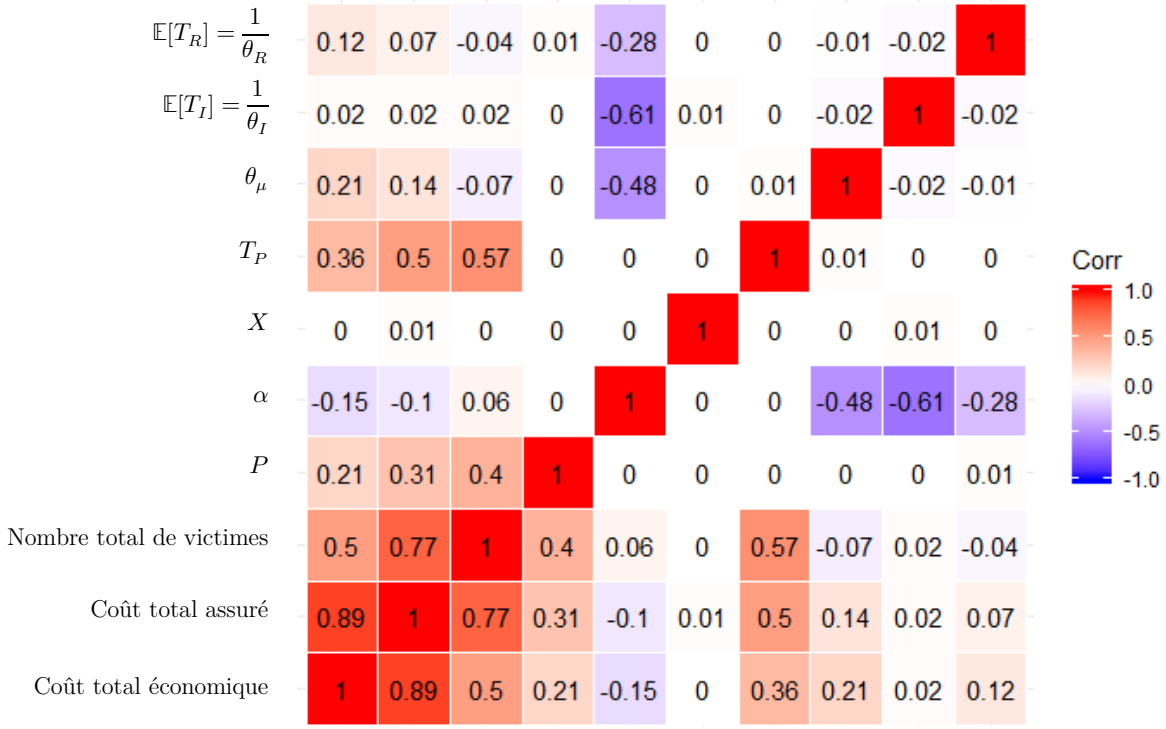


Figure 54 - Matrice de corrélation des variables du modèle

Les paramètres que nous avions estimés dans la section précédente ont bien entendu conservé leurs corrélations. En revanche, les corrélations des paramètres au coût et au nombre de victimes ont évolué avec l'introduction d'un aléa sur les hyper-paramètres. Le taux de transmission perd de son influence sur le nombre de victimes. Ce sont désormais la proportion d'entreprises vulnérables et le temps avant l'arrivée d'un patch qui dirigent principalement le nombre de victimes. Le coût de la rançon présente une corrélation nulle avec la perte : il contribue en effet très peu au coût simulé par h puisque nous avions supposés que la rançon était payée sur seulement 5% des ordinateurs.

Le nombre total de victimes est corrélé positivement au coût total assuré et au coût total économique, ce qui est cohérent. Nous avions en effet estimé les paramètres de telle sorte qu'un coût économique stable (NotPetya 875 millions et WannaCry 700 millions) soit atteint par peu ou beaucoup de victimes générées. Nous avions donc une corrélation quasi nulle entre le nombre de victimes et le coût total économique de l'évènement.

En rendant aléatoire la surface vulnérable et le temps de l'attaque, chaque type d'évènement peut être amplifié. On peut par exemple avoir une attaque de forte sévérité individuelle couplée à un grand nombre de victimes si les paramètres estimés autours de NotPetya sont associés à un long temps d'attaque et une plus grande proportion de vulnérables. Sur cet exemple, il va de soi que les paramètres de NotPetya associés à un temps d'attaque plus long feront plus de victimes et causeront plus de dégâts économiques, d'où l'apparition d'une corrélation positive entre le nombre total de victimes et le coût total.

L'aspect intéressant ici est la corrélation plus élevée du nombre de victimes à la perte totale assurée (0.77) qu'à la perte économique (0.5). La corrélation positive entre nombre de victimes et perte assurée signifie que plus l'évènement génère de victimes, plus la perte assurée sera importante. Une plus forte corrélation indique une plus grande dépendance de la perte assurée au nombre de victimes et donc au nombre de polices touchées. A perte économique égale, quel type d'évènement coûte le plus cher à notre portefeuille ?

Nous souhaitons vérifier que la forte corrélation positive n'est pas uniquement vraie pour un type d'évènement plus probable qui influence la covariance à la hausse. En effet pour V le nombre de victimes, $C_{assuré}$ et $C_{éco}$ les coûts assurés et économiques on a la relation suivante :
$Cov(V, C_{assuré}) = \sum_x Cov(V, C_{assuré} \ | C_{éco} = x) P(C_{éco} = x)$
Pour vérifier cela nous regardons nos simulations sur des fenêtres de 100 millions de coût. Le coût total étant rendu quasi stable sur ces fenêtres, ses corrélations avec d'autres variables seront proches de zéro. Sur chaque fenêtre nous allons nous intéresser à la corrélation du nombre de victimes avec la perte assurée. On obtient le graphique suivant :

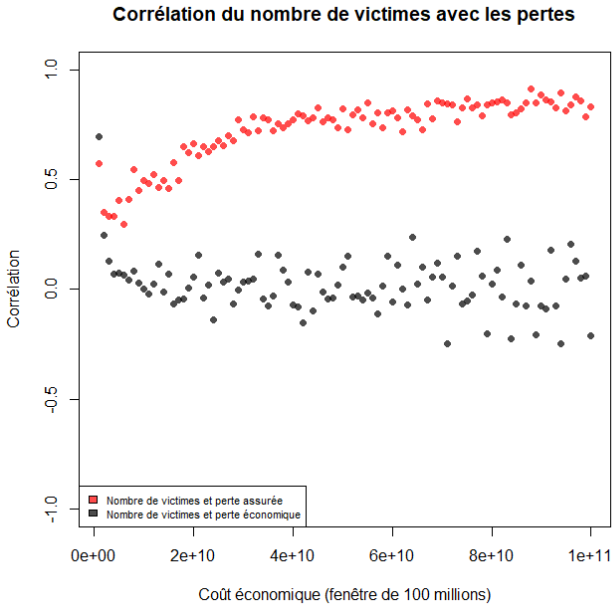


Figure 55 - Corrélation entre nombre de victimes et pertes (économiques et assurées) sur des fenêtres de 100 millions de perte

Pour chaque fenêtre d'observations, on note une corrélation positive. En procédant ainsi on vérifie bien que la corrélation est positive pour toutes les valeurs prises par le coût total. Il n'y a pas de fenêtre surpondérée qui influe sur la corrélation globale de l'échantillon, mais bien une corrélation positive pour toute valeur du coût total. Cela signifie donc que pour un coût total économique comparable, notre portefeuille supporte mieux une perte individuelle élevée qu'un grand nombre de victimes. On déduit donc la présence de limites assez prudentes dans les contrats.
On observe aussi une augmentation de la corrélation entre le coût assuré et le nombre de victimes lorsque la fenêtre du coût économique prend de plus grandes valeurs. Une augmentation du coût économique peut résulter d'une augmentation du nombre de victimes d'une part et d'une augmentation du coût par police d'autre part ou encore des deux combinées. Lorsque le coût par police augmente, les déductibles ne permettent plus qu'une victime supplémentaire engendre un coût assuré nul. Les évènements plus coûteux en perte économique comportent potentiellement une plus fort coût par police. Dans ces cas-là, les polices supplémentaires touchées auront plus facilement un coût économique dépassant les Déductibles, ce qui in fine engendrera une perte assurée, d'où une corrélation plus importante entre nombre de victimes et perte assurée pour les évènements dont le coût économique est plus élevé.

Il serait aussi intéressant de regarder l'influence des paramètres de sévérité sur la perte assurée. Pour cela on pourrait distinguer les simulations générées, selon l'appartenance des paramètres à l'ensemble qui engendrait une boule proche de NotPetya ou de WannaCry lors de l'estimation du modèle.

Afin d'illustrer l'intérêt de disposer de plusieurs scénarios dans le modèle interne, nous donnons pour chaque scénario la répartition moyenne de la perte économique totale par sous-garantie :

Sous-garantie	% de la perte dans le scénario ransomware	% de la perte dans le scénario cloud
BI	76%	0%
CBI	0%	46%
CRE	6%	0%
CYL	4%	11%
IRC	14%	26%
RLD	0%	17%

Figure 56 - Répartition de la perte économique en sous-garanties

Le scénario ransomware touche principalement la garantie BI, qui n'était pas impactée par le scénario cloud. Ce fort impact est cohérent avec notre étude de NotPetya : lors d'une attaque ransomware, les entreprises essuient principalement des pertes dues à l'impossibilité d'exercer une activité normale, ce qui provoque une forte perte de chiffre d'affaires et donc de bénéfices. La garantie CRE est elle aussi touchée contrairement au scénario cloud. On confirme donc l'intérêt d'avoir plusieurs scénarios pour compléter notre notre vision du risque porté par le portefeuille.

Maintenant que nous avons une certaine idée de la panoplie d'évènements générés par le modèle, intéressons-nous à la distribution du Destruction Rate (DR).

3.4.2.4 Distribution du DR

Regardons la valeur du DR à l'échelle du groupe AXA. Rappelons que le DR correspond à la perte totale assurée divisée par l'exposition totale (2.3.3). Il traduit la part de l'exposition qui est consommée par l'évènement. Il est donc équivalent d'étudier la perte assurée ou le DR à une constante multiplicative près.
Intéressons-nous tout d'abord à la convergence des estimateurs avant de présenter les résultats.

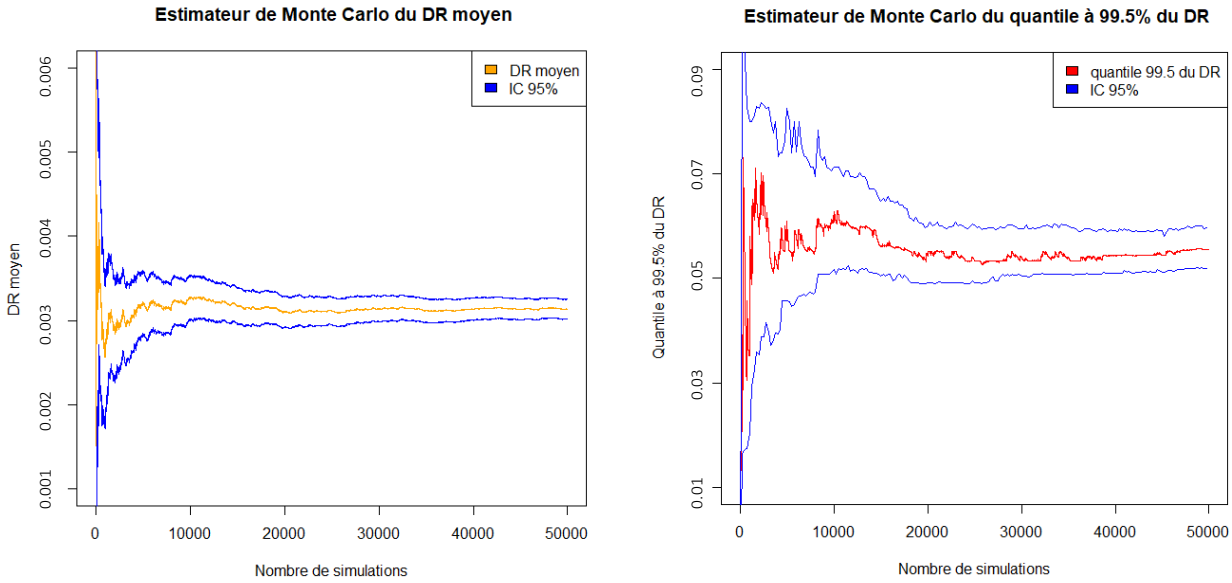


Figure 57 -Convergence des estimateurs de Monte Carlo

A gauche nous avons tracé l'estimateur de Monte Carlo du DR moyen avec son intervalle de confiance à 95% symétrique obtenu grâce au TCL. A droite nous avons tracé l'estimateur de Monte Carlo du quantile à 99.5% du DR avec son intervalle de confiance à 95% obtenu par bootstrap générique, et qui n'est ici pas symétrique. Les deux estimateurs sont quasi plats dès 40 000 simulations. Nous pouvons donc présenter ces estimateurs pour 50 000 simulations :

Nombre de simulations	Borne Inf IC 95%	Moyenne du DR par Monte Carlo	Borne Sup IC 95%
50 000	0.357%	0.366%	0.375%

Figure 58 - Estimateur de Monte Carlo du DR moyen

Nombre de simulations	Borne Inf IC 95%	Quantile à 99.5% du DR par Monte Carlo	Borne Sup IC 95%
50 000	5.84%	6.11%	6.4%

Figure 59 - Estimateur de Monte Carlo du quantile à 99.5% du DR

Le DR moyen est estimé à 0.366%, et se situe entre 0.357% et 0.375% avec une confiance de 95%.
Le quantile à 99.5% du DR est nettement plus élevé puisqu'il représente 16.7 fois le DR moyen soit 6.11%. Les bornes inférieures et supérieures de l'estimateur du quantile valent respectivement 5.84 et 6.4 pourcents. Traçons la distribution du DR avec son quantile à 99.5% en rouge :

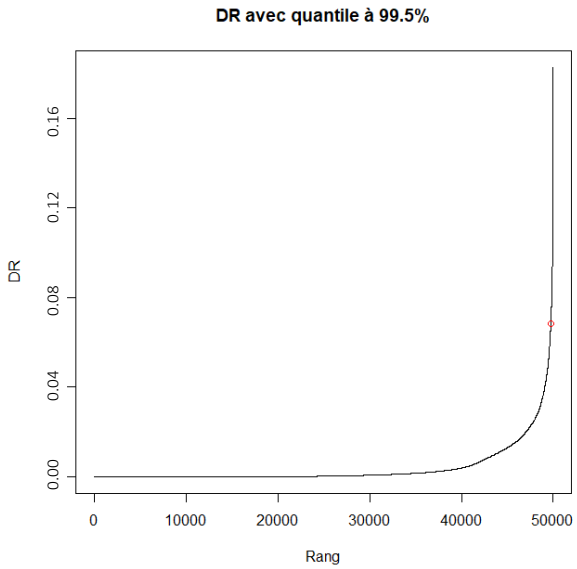


Figure 60 - Distribution du DR

On observe une fonction qui croit exponentiellement, ce qui est cohérent avec la description souvent donnée du risque cyber, à savoir un risque exponentiel. En effet, selon les motivations du hacker une attaque cyber peut toucher un à plusieurs milliers d'ordinateurs dans le monde entier et donc causer des petits dégâts isolés comme des dégâts simultanés très importants.

Nous avons obtenu le DR d'ordre 99.5% au niveau du groupe AXA. Le coût de chaque évènement peut être réparti entre les entités AXA en retraçant les polices touchées. Ainsi, nous obtenons le quantile à 99.5% du DR par entité (non présenté dans le mémoire). L'écart-type entre ces DR par entités est d'environ 20%, ce qui indique une certaine hétérogénéité entre les portefeuilles des différentes entités. Il est intéressant d'étudier d'où proviennent ces disparités. Pour cela, nous regardons les pertes par sous-garanties de chaque entité et calculons les fréquences auxquelles sont touchées les garanties ainsi que le coût moyen par sous-garantie.

Donnons ici un exemple d'étude. Nous remarquons qu'une entité présente un DR très élevé de 0.62. Étudions de plus près l'impact des évènements générés sur cette entité et regardons ensuite la structure du portefeuille pour juger la cohérence des résultats renvoyés par le modèle.

Pour cette entité, les garanties BI et CYL sont respectivement touchées par 12 et 16 pourcents des évènements générés par le modèle, ce qui est très peu. Les pertes moyennes (lorsque la sous-garantie est touchée) s'élèvent à 485 000 euros pour le BI et 78 000 euros pour le CYL. Les sous-garanties IRC et CRE ne comptabilisent aucune perte.
Regardons maintenant les garanties vendues par l'entité concernée. La limite moyenne de la sous-garantie BI est de 2.8 millions contre 2.4 millions pour la garantie CYL. Le portefeuille ne contient aucune sous-garantie IRC ni CRE, mais pour chaque police, les garanties BI et CYL sont souscrites.
Les polices concernent des entreprises dont le chiffre d'affaires journalier moyen s'élève à 12 millions d'euros. La garantie BI est donc très facilement consommable. Ce portefeuille est très concentré (moins de 10 polices) et contient deux très grandes entreprises et quelques entreprises de taille moyenne. Il suffit que l'une de ces deux très grandes entreprises soit touchée en même temps qu'une partie des entreprises de taille moyenne pour que le DR explose.

Sur cet exemple, on constate que le modèle pénalise fortement les portefeuilles concentrés sur des grandes entreprises si on s'intéresse uniquement au quantile de la perte à 99.5%. En effet, nous avons vu que les polices de l'entité A étaient rarement touchées (environ 15% du temps) mais lorsqu'elles le sont, les limites de couverture sont très vite atteintes. Nous avons donc un quantile du DR à 99.5% qui s'élève à 0.62 alors que le DR médian est de 0%.

3.4.2.5 Construction de l'ELT

Afin d'incorporer le scénario au modèle cyber, nous construisons une table contenant tous les évènements générés. Chaque ligne de la table correspond à un évènement tandis que les colonnes correspondent aux pertes assurées de chaque entité.
Il faudra ensuite estimer la fréquence d'occurrence d'une attaque ransomware et une éventuelle relation de dépendance avec une attaque de cloud afin de finaliser l'incorporation du scénario au modèle cyber. Le modèle cyber pourra tirer des évènements dans les ELT du scénario cloud et les ELT du scénario ransomware afin de construire des YLT et ainsi obtenir la distribution de la perte assurée annuelle relative au risque cyber.

3.5 Critique du modèle

Nous avons construit un nouveau scénario pouvant être incorporé au modèle interne cyber du groupe AXA. Il est maintenant temps d'évaluer notre approche, d'en donner les avantages et les faiblesses puis de proposer des travaux complémentaire contribuant tant à l'amélioration du modèle qu'à son étude.

3.5.1 Avantages du modèle

Construction du modèle
Le modèle élaboré au fil de ce mémoire a su tirer parti du peu de données disponibles pour construire un scénario le plus cohérent possible. Il permet de reproduire NotPetya et WannaCry ainsi que des variantes bien plus sévères grâce à une proportion d'entreprises vulnérables plus importante, une durée d'attaque plus longue et un coût de rançon plus élevé.

Apport du scénario dans le modèle interne AXA
Ce scénario permet d'apporter une certaine diversité par rapport au scénario cloud existant. Le scénario touche en effet des garanties différentes de celles concernées par le scénario cloud.
Les hypothèses et données servant à la construction du scénario proviennent de sources différentes de celles utilisées pour la construction du scénario cloud. Par exemple ici, l'influence du secteur sur le risque porté par chaque police est prise en compte via le nombre d'ordinateurs (obtenu à partir d'une base de l'OCDE). Les polices les plus exposées au risque sont celles dont les entreprises possèdent un parc important d'ordinateurs.
Le modèle permet d'avoir un évènement à l'échelle du groupe AXA, sans faire intervenir l'aspect géographique, en partie utilisé dans le scénario cloud. Il prend donc en compte le caractère systémique du risque à l'échelle mondiale.

Évolution des paramètres
La méthode d'estimation présentée peut être reconduite si d'autres évènements ont lieu ou si un évènement fictif reflétant les craintes futures était envisagé. Il suffirait d'ajouter une cible et si nécessaire de retravailler la structure la fonction de coût.

3.5.2 Limites du modèle

Méthode d'estimation
L'estimation des lois *a posteriori* s'effectue conditionnellement aux entreprises présentes dans le portefeuille. En effet, nous avions vu que le support de Z dépendait du portefeuille. Cette démarche est donc cohérente pour des portefeuilles représentant assez bien l'économie mondiale, c'est-à-dire suffisamment grands et diversifiés en termes de tailles d'entreprises et de secteurs d'activité, ce qui est le cas du portefeuille regroupant tous les contrats cyber des entités AXA.
Nous ne recommandons pas de procéder ainsi pour des petits portefeuilles. Par exemple, pour un petit portefeuille composé uniquement de grandes entreprises la perte aurait tendance à exploser : la cible $\eta(y)$ pourrait par conséquent être hors d'atteinte. Au contraire, un portefeuille constitué uniquement de très petites entreprises ne parviendra pas à générer une perte comparable à celle de NotPetya.

Précision du modèle
De nombreux proxies sont utilisés (nombre d'ordinateurs, nombre de serveurs) et contribuent donc à diminuer la précision du modèle. Malgré l'utilisation de données incomplètes, le modèle donne un ordre de grandeur cohérent et présente un aspect du risque cyber souvent évoqué : l'aspect exponentiel de ce risque. La distribution de la perte assurée obtenue présente en effet une moyenne très éloignée du quantile à 99.5%, traduisant l'explosion du coût sur certains évènements. De plus amples recherches permettraient aussi d'affiner la structure de la fonction de coût h et ainsi accroitre la précision du modèle.

Capacité à prédire l'impact d'une attaque en cours
En proposant une analogie entre cyber et pandémie nous devons évaluer l'utilité du modèle sur sa capacité prédictive. Les modèles épidémiologiques sont utilisés en assurance pour simuler l'impact de pandémies sur le portefeuille d'assurés. De manière plus générale, lorsqu'une épidémie se dessine, les modèles épidémiologiques servent à anticiper la potentielle transformation de l'épidémie en pandémie. L'objectif étant d'endiguer l'épidémie en prenant les mesures sanitaires nécessaires (vaccins, quarantaines etc.) pour éviter une propagation vers d'autres zones géographiques. Pour ce faire, lorsqu'un nouveau virus apparaît et est susceptible d'engendrer une pandémie, les paramètres du modèle sont estimées sur la population se trouvant dans la zone géographique de l'épidémie. Ainsi, le temps nécessaire à l'épidémie pour se propager peut-être évalué et les mesures nécessaires peuvent être prises. Les modèles épidémiologiques sont donc aussi utilisables en même temps que se dessine une épidémie.
Les propagations de NotPetya et WannaCry étaient si fulgurantes qu'elles laissent très peu de temps pour évaluer le taux de transmission du virus et prévoir la taille finale de l'attaque. A ce jour, le patient zéro et ses contacts précis sont encore incertains. Si une nouvelle attaque informatique avait lieu, sachant le système informatique attaqué, l'assureur pourrait très vite établir une borne supérieure du nombre de victimes pouvant être impactées au sein de son portefeuille. La durée de l'attaque pourrait aussi lui donner une indication quant au nombre de victimes potentiellement touchées au sein de son portefeuille et lui permettre in fine d'établir une borne supérieure de la perte totale assurée.

3.5.3 Travaux complémentaires et pistes d'amélioration

Tester les hypothèses et effectuer des sensibilités

Il serait intéressant d'étudier l'impact de l'utilisation d'autres familles de lois de durées pour les temps infectieux, de réparation et de temps avant l'arrivée d'un patch.

Nous avons montré de manière qualitative l'impact des variables rendues aléatoires lors de la simulation. Des études de sensibilité plus approfondies pourraient être faites sur le modèle.

Lors de l'intégration d'un portefeuille de coassurance, nous avions montré que le modèle cloud était peu sensible au chiffre d'affaires des assurés. Le chiffre d'affaires intervenant clairement dans le calcul du coût associé à la sous-garantie BI, il serait intéressant d'étudier la dépendance du scénario ransomware à cette variable.

Données

Les données manquantes sur les assurés (comme le nombre d'ordinateurs, le type de système d'exploitation utilisé) pourraient être remplies facilement lors de l'enrichissement des bases de données. Il sera alors intéressant de voir l'évolution des résultats.

Une fois que les données le permettront, nous pourrions prendre en comptes les profils informatiques des entreprises et des scores de risque associés aux entreprises.

On distinguerait alors deux niveaux d'ajustement possibles :

-au niveau des entreprises, le score de risque de chaque entreprise peut influencer le taux de transmission du virus. Une entreprise avec un bon score serait moins fréquemment contaminée. Ainsi, le portefeuille serait touché plus souvent sur les entreprises de mauvais de score. Les pertes concerneraient donc plus fréquemment les 'mauvais' risques et le modèle pénaliserait donc les 'mauvais' risques dont l'exposition est trop importante.

-au niveau global : quelle part du risque porte AXA ? Nous avions fait l'hypothèse qu'AXA subissait 10% de NotPetya ou WannaCry pour estimer les paramètres du modèle, ces 10% correspondant à la part de marché d'AXA sur les contrats cyber. En incorporant les scores de risque des assurés, il faudrait étudier si le portefeuille AXA porte finalement plus ou moins de risque que la moyenne. Détenir 10% du marché ne signifie pas pour autant détenir 10% du risque.

Conclusion

Dans ce troisième et dernier chapitre, nous avons tout d'abord justifié l'analogie entre risque cyber et risque de pandémie avant de nous familiariser avec les modèles épidémiologiques compartimentaux.

Nous avons ensuite construit un modèle statistique permettant de générer des observations synthétiques d'une attaque ransomware. Nous avons choisi d'incorporer un modèle SIR adapté à notre modèle ransomware pour générer des victimes munies de leurs temps infectieux, temps de réparation et sévérités individuelles. Une fois ces victimes et leurs caractéristiques obtenues, nous avons construit une fonction h permettant d'associer à chaque victime un coût économique réparti en garanties. La construction de cette fonction a été faite en s'appuyant sur les données recensées sur NotPetya.

Nous avons utilisé le cadre bayésien pour mettre à profit nos connaissances et estimer la lois *a posteriori* des paramètres du modèle. Nous avons montré que la méthode MCMC n'était pas adaptée à notre problème avant d'introduire la méthode ABC. ABC permet de nous affranchir du calcul de la vraisemblance du modèle, dont l'espace de grande dimension rend difficile le calcul, et de pallier l'absence d'observation complètement observées d'attaques ransomware. Nous estimons la loi *a posteriori* des paramètres du modèle lorsqu'une transformation statistique $\eta(z)$ de nos observations est

proche d'une transformation statistique d'un évènement réel : NotPetya. Pour procéder à ces estimations, les hyper-paramètres du modèle sont fixées à leur valeur connue pour NotPetya (durée de l'attaque, proportion de vulnérables et coût de la rançon).
Nous avons ensuite proposé 3 jeux de lois *a priori* induisant 3 modèles statistiques différents. Nous nous sommes intéressés à la loi *a posteriori* de chacun de ces 3 modèles et aux avantages et inconvénients induits par chacun de ces modèles. Le dernier modèle permettant de reproduire NotPetya et WannaCry ainsi que des évènements entre ces deux attaques a finalement été choisi puisqu'il permet de générer des évènements de nature variée.
Pour générer des évènements et étudier la distribution de la perte assurée, nous avons procédé par bootstrap sur les paramètres acceptés afin de simuler les paramètres du modèle selon leur loi *a posteriori* et avons rendu aléatoires les hyper-paramètres du modèle. Nous avons analysé l'impact de l'aléa introduit sur ces hyper-paramètres, et avons étudié les évènements générés par le modèle. Nous avons ensuite présenté la distribution de la perte assurée et calculé le quantile à 99.5% de la perte assurée à l'échelle du groupe AXA et de chacune de ses entités.
Enfin, nous avons expliqué comment ce scénario pourrait être intégré au modèle interne cyber et avons dressé les avantages et inconvénients du modèle et proposé des pistes d'amélioration.

Conclusion

Ce mémoire avait pour principal objectif la construction d'un scénario d'accumulation permettant de compléter la vision du risque porté par AXA sur l'ensemble de ses contrats cyber *affirmative First Party.*

Pour y parvenir, nous avons tout d'abord étudié le risque en tant que tel à travers des exemples et avons déduit ses principales caractéristiques. Nous retiendrons que le risque cyber est un risque *man made* de nature évolutive, systémique et imprévisible.

A travers l'intégration au modèle cloud d'un portefeuille de coassurance et l'implémentation de l'attaque Bashe, nous avons montré que la répartition des sous-couvertures de notre portefeuille et le choix des sous-couvertures impactées par le scénario influençaient la distribution de la perte assurée. Ces éléments ont motivé la mise en place d'un scénario supplémentaire pour compléter notre vision du risque porté par le portefeuille du groupe AXA.

Les caractéristiques du risque cyber nous ont incités à proposer un parallèle de modélisation avec le risque de pandémie pour simuler la propagation d'un ransomware. Nous avons adapté un modèle SIR au risque cyber et estimé les paramètres de notre modèle en nous appuyant sur NotPetya et WannaCry. Pour cela, nous avons recensé des informations sur ces deux attaques. Les données récoltées étant parcimonieuses, nous avons utilisé le cadre bayésien pour mettre à profit nos connaissances acquises sur ces évènements et incorporer une notion d'incertitude sur les paramètres du modèle. Pour l'estimation des paramètres, nous avons placé le modèle dans des conditions similaires à celles connues pour NotPetya et WannaCry. Les paramètres du modèle final choisi ont été estimés de manière à pouvoir simuler des évènements de natures diverses : des évènements de forte sévérité individuelle et de faible portée (NotPetya), des évènements de moins grande sévérité individuelle et de plus grande portée (WannaCry), ou bien des évènements centraux nouveaux mais vraisemblables puisqu'ils se situent entre NotPetya et WannaCry. En nous affranchissant des conditions d'estimation propres à ces deux évènements, le modèle est en mesure de générer d'autres évènements catastrophes vraisemblables et de plus grande sévérité. La distribution de la perte par évènement induite par le scénario ransomware illustre une caractéristique propre au risque cyber : sa dimension exponentielle.
Le modèle ainsi construit répond à nos attentes initiales dans la mesure où il permet de générer des évènements d'accumulation apportant une certaine diversité par rapport au scénario cloud existant. Il complète donc la vision du risque cyber porté par notre portefeuille.

Pour finaliser l'intégration du scénario ransomware au modèle interne cyber, il reste à estimer la fréquence annuelle d'occurrence d'attaques ransomware et une éventuelle dépendance avec le scénario cloud. Des tests de sensibilité plus poussés pourraient être faits pour compléter l'étude du modèle. Il serait aussi intéressant de suivre l'impact de l'enrichissement de la qualité des données sur le calcul de la perte assurée et d'étudier les différentes façons de prendre en compte des scores de risque sur les assurés lorsque ces informations seront disponibles.

Bibliographie

[1] APREF, «Etude sur les "cyber risques" et leur (ré) assurabilité,» Juin 2016.

[2] B. CHABRIER, «le cyber, première menace pour l'assurance,» 6 Février 2019. [En ligne]. Available: https://www.argusdelassurance.com/les-assureurs/le-cyber-premiere-menace-pour-les-risk-managers-amrae-2019.141835.

[3] S. G. P&C, «Cyber Risk Insurance Introduction, Campus 2018,» 2018.

[4] B. VENARD, «Equifax: un piratage qui donne des sueurs froides,» 30 Novembre 2017. [En ligne]. Available: https://www.lesechos.fr/idees-debats/cercle/equifax-un-piratage-qui-donne-des-sueurs-froides-1010045.

[5] P. COLLINSON, «Visa admits 5m payments failed over a broken switch,» 19 Juin 2018. [En ligne]. Available: https://www.theguardian.com/money/2018/jun/19/visa-admits-5m-payments-failed-over-a-broken-switch.

[6] L. SYED, «Mémoire d'Actuariat - Élaboration d'un modèle d'accumulation du risque cyber "stand alone first party" en Europe,» 2018.

[7] F. PONS, «Mémoire d'Actuariat - Etude Actuarielle du Cyber-Risque,» 2014.

[8] R. BOULLE, «Denis Kessler (Scor) : « Le risque cyber, aussi important que le risque de catastrophes naturelles »,» mai 2019. [En ligne]. Available: https://www.argusdelassurance.com/acteurs/reassureurs/denis-kessler-scor-le-risque-cyber-aussi-important-que-le-risque-de-catastrophes-naturelles.147130.

[9] «European Union Agency for Cyber Security,» 2019. [En ligne]. Available: https://www.enisa.europa.eu/media/enisa-en-francais/.

[10] «Directive Network and Information System Security,» [En ligne]. Available: https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/.

[11] Lloyds, «CyRim Report 2019 - Bashe attack Global infection by contagious malware,» 2019.

[12] Insitut Ponemon, «2018 Cost of a Data Breach Study : Global Overview,» 2018.

[13] S. PATON, «3 attaques de social engineering auxquelles vous n'auriez jamais pensé,» mai 2014. [En ligne]. Available: https://www.institut-pandore.com/hacking/3-attaques-social-engineering/.

[14] L. THEVENIN, «Le marché de la cyberassurance promis à une croissance rapide,» Septembre 2018. [En ligne]. Available: https://www.lesechos.fr/finance-marches/banque-assurances/le-marche-de-la-cyberassurance-promis-a-une-croissance-rapide-139597.

[15] SWISSRE, «L'assurance dans le monde en 2017,» 2018. [En ligne]. Available: https://www.swissre.com/dam/jcr:0483f88f-e7a2-47ab-bcf4-37cd4682da19/nr_20180705_sigma_3_2018_fr.pdf.

[16] L. THEVENIN, «La cyberassurance gagne du terrain sur fond de montée du risque,» Février 2019. [En ligne]. Available: https://www.lesechos.fr/finance-marches/banque-assurances/la-cyberassurance-gagne-du-terrain-sur-fond-de-montee-du-risque-962307.

[17] L. THEVENIN, «Comment AXA veut accéléer sur la cyber assurance,» Juin 2018. [En ligne]. Available: https://www.lesechos.fr/2018/06/comment-axa-veut-accelerer-sur-la-cyber-assurance-991852.

[18] S. ARYAL, «differences-between-antigenic-shift-and-antigenic-drift,» Juin 2018. [En ligne]. Available: https://microbiologyinfo.com/differences-between-antigenic-shift-and-antigenic-drift/.

[19] R. SPEISSER, «Mémoire d'Actuariat - Evaluation du risque de pandémie et construction de deux modèles internes partiels en assurance de personnes dans le cadre de Solvabilité II,» 2013.

[20] K. HADDAD, «Mémoire d'Acturiat - Risque de pandémie en réassurance,» 2018.

[21] W. HAMER, «The Milroy lectures on epidemic disease in England: the evidence of variability and of persistency of type,» Bedford Press, 1906.

[22] MCKENDRICK et KEMARCK, «A Contribution to the Mathematical Theory of Epidemics.,» Proceedings of the Royal Society of London, 1927.

[23] A. P.ERFÖS, «The Evolution of Random Graphs,» Institute of Mathematics, Hungarian Academy of Sciences, 1960.

[24] O. BOITET, «Cyber attaque mondiale après wannacry notpetya piege 2000 entreprises,» Juin 2017. [En ligne]. Available: http://www.leparisien.fr/high-tech/cyberattaque-mondiale-apres-wannacry-notpetya-piege-2000-entreprises-28-06-2017-7093677.php.

[25] R. SOBERS, «60 Must-Know Cybersecurity Statistics for 2019,» Avril 2019. [En ligne]. Available: https://www.varonis.com/blog/cybersecurity-statistics/.

[26] R. BRANDOM, «It's already too late for today's ransomware victims to pay up and save their computers,» Juin 2017. [En ligne]. Available: https://www.theverge.com/2017/6/27/15881110/petya-notpetya-paying-ransom-email-blocked-ransomware.

[27] M. SAMPSON, «DLA piper NotPetya,» Mai 2018. [En ligne]. Available: https://michaelsampson.net/2018/05/12/dla-piper-notpetya/.

[28] A. GREENBERG, «The Untold Story of NotPetya, the Most Devastating Cyberattack in History,» Septembre 2018. [En ligne]. Available: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

[29] E. LAFORE, L. MERINE et V. LEMENUT, «Risk insight - Cyber Resilience un nouveau pillier de la stratégie cybersécurité,» 2018. [En ligne]. Available: https://www.wavestone.com/app/uploads/2018/01/2019-RiskInsight-VE.pdf.

[30] R. CROZIER, «DLA Piper paid 15,000 hours of IT overtime after NotPetya attack,» Mai 2018. [En ligne]. Available: https://www.itnews.com.au/news/dla-piper-paid-15000-hours-of-it-overtime-after-notpetya-attack-490495.

[31] C. DE., «Trois cyber-incidents qui font froid dans le dos,» Février 2018. [En ligne]. Available: https://www.lesechos.fr/2018/02/trois-cyber-incidents-qui-font-froid-dans-le-dos-967295.

[32] C. AUFFRAY, «Les 10 nuits en enfer de Maersk pour réinstaller 4000 serveurs et 45000 PC,» Janvier 2018. [En ligne]. Available: https://www.zdnet.fr/actualites/les-10-nuits-en-enfer-de-maersk-pour-reinstaller-4000-serveurs-et-45000-pc-39863304.htm.

[33] A. SATARIANO et N. PERLROTH, «Big Companies Thought Insurance Covered a Cyberattack. They May Be Wrong,» Avril 2019. [En ligne]. Available: https://www.nytimes.com/2019/04/15/technology/cyberinsurance-notpetya-attack.html.

[34] M. UNTERSINGER, «Comment fonctionne Petya, le virus qui a touché de nombreuses très grandes entreprises ?,» Juin 2017. [En ligne]. Available: https://www.lemonde.fr/pixels/article/2017/06/28/comment-fonctionne-petya-le-virus-qui-a-touche-de-nombreuses-tres-grandes-entreprises_5152547_4408996.html.

[35] M. LEHOT, «Cyber risques: les assureurs se plient en quatre,» Septembre 2017. [En ligne]. Available: https://www.argusdelassurance.com/acteurs/cyber-risques-les-assureurs-se-plient-en-quatre.121930.

[36] E. PROTALINSKI, «Net Applications: Windows 10 passes Windows 7 in market share,» Janvier 2019. [En ligne]. Available: https://venturebeat.com/2019/01/01/net-applications-windows-10-passes-windows-7-in-market-share/.

[37] «La prise en charge de windows 7 pendra fin le 14 janvier 2020,» Juin 2019. [En ligne]. Available: https://support.microsoft.com/fr-fr/help/4057281/windows-7-support-will-end-on-january-14-2020.

[38] «Analyzing Ponemon Cost of Data Breach,» Décembre 2014. [En ligne]. Available: https://datadrivensecurity.info/blog/posts/2014/Dec/ponemon/.

[39] OECD, «Accès et utilisation des TIC par les entreprises,» Juillet 2019. [En ligne]. Available: https://stats.oecd.org/viewhtml.aspx?datasetcode=ICT_BUS&lang=fr.

[40] A. C. R. Inc, «Identifying IT Markets and Market Size,» 2011.

[41] B. GILL, «What is the typical cost of recovering data per GB?,» 2015. [En ligne]. Available: https://www.quora.com/What-is-the-typical-cost-of-recovering-data-per-GB.

[42] E. THOMPSON, «How Much Should a Business Computer Cost?,» Juin 2017. [En ligne]. Available: https://www.business.org/finance/cost-management/much-computer-cost/.

[43] J.-M. MARIN, P. PUDLO, C. P.ROBERT et R. J.RYDER, «Approximate Bayesian computational methods,» 2011.

[44] C. T. QUORA, «How Similar Are WannaCry And Petya Ransomware?,» Juin 2017. [En ligne]. Available: https://www.forbes.com/sites/quora/2017/07/05/how-similar-are-wannacry-and-petya-ransomware/#1849446e46eb.

[45] V. ABRIAL, «La cyber assurance devient une priorité pour les dirigeants d'entreprises,» Janvier 2015. [En ligne]. Available: https://www.latribune.fr/loisirs/la-tribune-now/20150128tribd355efe7a/la-cyber-assurance-devient-une-priorite-pour-les-dirigeants-d-entreprise.html.

[46] L. THEVENIN, «Le marché de la cyberassurance promis à une croissance rapide,» Septembre 2018. [En ligne]. Available: https://www.lesechos.fr/finance-marches/banque-assurances/le-marche-de-la-cyberassurance-promis-a-une-croissance-rapide-139597.

Annexes

A Quelques lois usuelles

Lois discrètes

Loi	Paramètres	$P(X=k)$	$\mathbb{E}[X]$	$\mathbb{V}[X]$	support
Bernoulli	$p \in [0,1]$	$p^k(1-p)^{1-k}$	p	$p(1-p)$	$\{0,1\}$
Équiprobable		$1/n$	$\frac{n+1}{2}$	$\frac{n^2+1}{12}$	$\{1,2,\dots n\}$
Binomiale	$n \in \mathbb{N}^*, p \in [0,1]$	$C_n^k p^k (1-p)^{n-k}$	np	$\mathrm{np}(1-\mathrm{p})$	$\{0,1,\dots n\}$
Géométrique	$p \in [0,1]$	$p(1-p)^{k-1}$	$\frac{1}{p}$	$\frac{1-p}{p^2}$	$\mathbb{N}^*$
Poisson	$\lambda > 0$	$\frac{\lambda^k}{k!}e^{-\lambda}$	λ	λ	$\mathbb{N}$
Binomiale négative	$r \in \mathbb{N}^*, p \in [0,1]$	$C_{k+r-1}^k p^r (1-p)^k$	$\frac{r(1-p)}{p}$	$\frac{r(1-p)}{p^2}$	$k \geq r$

Lois continues

Loi	Paramètres	Densité $f(x)$	$\mathbb{E}[X]$	$\mathbb{V}[X]$	support
Exponentielle	$\lambda > 0$	$\lambda e^{-\lambda x}\mathbb{1}_{[0,\infty[}(x)$	$\frac{1}{\lambda}$	$\frac{1}{\lambda^2}$	$\mathbb{R}_+$
Gamma	$\alpha > 0, \beta > 0$	$\frac{\beta^\alpha}{\Gamma(\alpha)} x^{\alpha-1} e^{-\beta x}\mathbb{1}_{[0,\infty[}(x)$	$\frac{\alpha}{\beta}$	$\frac{\alpha}{\beta^2}$	$\mathbb{R}_+$
Normale	$\mu \in \mathbb{R}\ , \sigma^2 > 0$	$\frac{1}{\sqrt{2\pi}}\ \exp\ (-\frac{1}{2}(\frac{x-\mu}{\sigma})^2)$	μ	σ^2	$\mathbb{R}$
Weibull	$\lambda > 0, k > 0$	$\frac{k}{\lambda}\left(\frac{x}{\lambda}\right)^{k-1} \exp\ (-\left(\frac{x}{\lambda}\right)^k)$	$m = \lambda\Gamma(1+\frac{1}{k})$	$\lambda^2\Gamma\left(1+\frac{1}{k}\right) - \ m^2$	$\mathbb{R}_+$
Beta	$a > 0, b > 0$	$\frac{\Gamma(\mathrm{a}\ +\ \mathrm{b})}{\Gamma(a)\Gamma(b)} x^{a-1}(1-x)^{b-1}\mathbb{1}_{[0,1]}(x)$	$\frac{a}{a+b}$	$\frac{ab}{(a+b)^2(a+b+1)}$	$[0,1]$
Uniforme	$a < b$	$\frac{1}{b-a}\mathbb{1}_{[a,b]}(x)$	$\frac{a+b}{2}$	$\frac{(b-a)^2}{12}$	$[a,b]$

B Rappels de méthodes de simulations

Définition de l'inverse généralisée

Soit X une variable aléatoire réelle de fonction de répartition F . On appelle inverse généralisé (ou fonction quantile) de F , noté F^{-1} , la fonction définie pour tout $u \in [0\ ,\ 1]$ par :

$$F^{-1}(u) = inf\{x\ \in R :\ F(x) \geq u\}$$

Méthode d'inversion

Soit X une variable aléatoire réelle de fonction de répartition F et $U \sim U\ (0\ ,\ 1)$. Alors $F^{-1}(U)$ suit la loi de X . Il suffit donc de simuler u suivant $U\ (0\ ,1)$ puis d'appliquer la transformation $x = F^{-1}(u)$ pour simuler suivant la loi de X.

Preuve :Il s'agit alors de montrer que $F^{-1}(U)$ et X ont même fonction de répartition, i.e., pour tout y réel $P(F^{-1}(U) \leq y) = P(X \leq y) = F(y) = P(U \leq F(y))$

Il suffit donc de monter que pour tout y réel et tout u dans [0, 1],

$\{(u,y)$: $F^{-1}(u) \leq u\ \} = \{(u,y) : u \leq \mathrm{F}\ (\ y\ )\ \}$

($\subseteq$) Soit (u,y) tel que $F^{-1}(u) \leq y$. Par croissance de F, on a F $(F^{-1}(u) \leq \mathrm{F}(y)$. Et par définition de

l'inverse généralisée F ($F^{-1}(u)$) $\geq u$. D'où $u \leq F(y)$.
($\supseteq$) Soit (u, y) tel que $u \leq F(y)$. F^{-1} étant croissante, on a $F^{-1}(u) \leq F^{-1}\big(F(y)\big)$. La définition de l'inverse généralisée et la croissance de la fonction de répartition permettent d'écrire
$F^{-1}\{F(y)\} = inf\{x \in R : F(x) \geq F(y)\} = inf\{x \geq y : F(x) \geq F(y)\}$
On en déduit $F^{-1}\{F(y)\} \leq y$. Et donc $F^{-1}(u) \leq F^{-1}\{F(y)\} \leq y$.

Méthode de rejet
Soit X une variable de $\mathbb{R}^d$ que l'on souhaite simuler et dont la densité f est appelée densité cible, supposée connue à une constante multiplicative près. On note g la densité d'une variable aléatoire simple que l'on sait simuler, appelée densité candidate et qui satisfait :
$f(x) \leq Mg(x),\ x \in \mathbb{R}^d$ et $M \geq 1$ une constante.
Algorithme de rejet :

1. Générer $U \sim U(0\ ,1)$
2. Générer $Y \sim g$
3. Accepter $X = Y$ si $U \leq \frac{f(Y)}{Mg(Y)}$. Sinon rejeter et reprendre à l'étape 1.

Montrons que l'échantillon obtenu avec l'algorithme de rejet suit bien la loi de X. On passe par la fonction de répartition qui caractérise la loi :
Avec Bayes on a :

$$P(X \leq x\ |U \leq \frac{f(Y)}{Mg(Y)}) = \frac{P(Y \leq x, U\ \leq f(Y)/Mg(Y))}{P(U \leq \frac{f(Y)}{Mg(Y)})}$$

$$\begin{aligned} &= \frac{\int_{-\infty}^{x} P\big(U \leq \frac{f(y)}{Mg(y)}\big) g(y)dy}{\int_{-\infty}^{\infty} P\big(U \leq \frac{f(y)}{Mg(y)}\big) g(y)dy} \\ &= \frac{\int_{-\infty}^{x} \frac{f(y)}{Mg(y)} g(y)dy}{\int_{-\infty}^{\infty} \frac{f(y)}{Mg(y)} g(y)dy} \\ &= \int_{-\infty}^{x} f(y)dy \end{aligned}$$

Théorème Central Limite (TCL) :
Soit $X_1, \ldots, X_n$ une suite de variables iid, avec $\mathbb{E}(X_1) = m$ et $\mathbb{V}(X_1) = \sigma^2 < \infty$.
Notons $\overline{X_n} = \frac{1}{n}\sum_{i=1}^{n} X_i$
Alors : $\sqrt{n}\frac{\overline{X_n} - m}{\sigma} \overset{loi}{\rightarrow} Z$ avec $Z \sim N(0,1)$

Loi forte des grands nombres
Soit $X_1, \ldots, X_n$ une suite de variables iid, avec $\mathbb{E}(X_1) = m < \infty$
Alors : $\overline{X_n} \overset{p.s.}{\rightarrow} m$

Continuous mapping theorem
Soit g une fonction continue.
Si $X_n \overset{p.s}{\rightarrow} X$ alors $g(X_n) \overset{p.s}{\rightarrow} g(X)$
Si $X_n \overset{P}{\rightarrow} X$ alors $g(X_n) \overset{P}{\rightarrow} g(X)$
Si $X_n \overset{loi}{\rightarrow} X$ alors $g(X_n) \overset{loi}{\rightarrow} g(X)$

Lemme de Slutsky

Si $X_n \overset{loi}{\to} X$ et $Y_n \overset{P}{\to} c$ une constante, alors $(X_n, Y_n) \overset{loi}{\to} (X, c)$

Si $X_n \overset{loi}{\to} X$ et $Y_n \overset{P}{\to} c$ une constante, alors $X_n Y_n \overset{loi}{\to} Xc$

Intervalle de confiance de la perte moyenne d'un modèle

Pour obtenir un intervalle de confiance à 95% de la perte moyenne, on utilise le TCL associé au lemme de Slutsky.

La perte assurée générée par nos modèles est une variable aléatoire positive majorée par l'exposition totale de nos polices. Elle est bornée donc de carré intégrable. Soit $X_1, \dots, X_n$ une suite de pertes assurées simulées selon un même modèle statistique, avec $\mathbb{E}(X_1) = m$ et $\mathbb{V}(X_1) = \sigma^2 < \infty$. On peut appliquer le TCL : $\sqrt{n}\frac{\overline{X_n}-m}{\sigma} \overset{loi}{\to} Z$ avec $Z \sim N(0,1)$

On sait que la variance empirique converge en probabilité vers la variance théorique (obtenu via la loi des grands nombres et le continuous mapping theorem). La fonction racine carrée étant continue sur $\mathbb{R}^+$, elle est donc mesurable. Par conséquent, la racine carrée de la variance empirique converge en probabilité vers l'écart-type théorique. Notons $\widehat{\sigma_n}$ l'estimateur empirique de l'écart-type.

On a $\frac{\sigma}{\widehat{\sigma_n}} \overset{P}{\to} 1$

On applique Slutsky : $\sqrt{n}\frac{\overline{X_n}-m}{\sigma}\frac{\sigma}{\widehat{\sigma_n}} = \sqrt{n}\frac{\overline{X_n}-m}{\widehat{\sigma_n}} \overset{loi}{\to} Z$ avec $Z \sim N(0,1)$

L'intervalle de confiance de m est $[\overline{X_n} - q_{97.5\%}\frac{\widehat{\sigma_n}}{\sqrt{n}}, \overline{X_n} + q_{97.5\%}\frac{\widehat{\sigma_n}}{\sqrt{n}}]$, avec $q_{97.5\%}$le quantile à 97.5% d'une loi normale centrée réduite.

D Tables issues de CyRim

Sector	SVS	Premier	Large	Medium	Small
Business & Professional Services	3	8,00%	6,00%	6,00%	8,00%
Defense / Military Contractor	1	6,00%	4,00%	4,00%	3,00%
Education	5	16,00%	11,00%	11,00%	15,00%
Energy	2	6,00%	5,00%	5,00%	6,00%
Entertainment & Media	4	10,00%	8,00%	8,00%	10,00%
Finance - Banking	5	16,00%	11,00%	11,00%	15,00%
Finance - Insurance	4	10,00%	8,00%	8,00%	10,00%
Finance - Investment Management	4	11,00%	8,00%	8,00%	10,00%
Food & Agriculture	2	6,00%	5,00%	5,00%	6,00%
Healthcare	4	11,00%	8,00%	8,00%	10,00%
IT - Hardware	4	12,00%	8,00%	8,00%	10,00%
IT - Services	4	10,00%	8,00%	8,00%	10,00%
IT - Software	4	10,00%	8,00%	8,00%	10,00%
Manufacturing	4	10,00%	8,00%	8,00%	10,00%
Mining & Primary Industries	1	5,00%	2,00%	2,00%	3,00%
Pharmaceuticals	1	6,00%	3,00%	2,00%	3,00%
Real Estate / Property / Construction	4	11,00%	8,00%	8,00%	10,00%
Retail	5	14,00%	10,00%	10,00%	13,00%
Telecommunications	2	8,00%	5,00%	5,00%	6,00%
Tourism & Hospitality	3	9,00%	6,00%	6,00%	8,00%
Transportation / Aviation / Aerospace	4	10,00%	8,00%	8,00%	10,00%
Utilities	2	7,00%	5,00%	5,00%	6,00%

Tableau 44- Ratios de réplication S2

Sector	SVS	Premier	Large	Medium	Small
Business & Professional Services	3	12,00%	11,00%	8,00%	8,00%
Defense / Military Contractor	1	6,00%	4,00%	4,00%	5,00%
Education	5	21,00%	10,00%	15,00%	15,00%
Energy	2	8,00%	8,00%	6,00%	6,00%
Entertainment & Media	4	15,00%	14,00%	10,00%	10,00%
Finance - Banking	5	21,00%	20,00%	15,00%	15,00%
Finance - Insurance	4	14,00%	14,00%	10,00%	10,00%
Finance - Investment Management	4	14,00%	14,00%	10,00%	10,00%
Food & Agriculture	2	9,00%	8,00%	6,00%	6,00%
Healthcare	4	14,00%	14,00%	10,00%	10,00%
IT - Hardware	4	18,00%	13,00%	10,00%	10,00%
IT - Services	4	17,00%	14,00%	10,00%	11,00%
IT - Software	4	14,00%	14,00%	10,00%	10,00%
Manufacturing	4	14,00%	14,00%	10,00%	10,00%
Mining & Primary Industries	1	6,00%	4,00%	3,00%	3,00%
Pharmaceuticals	1	6,00%	4,00%	3,00%	4,00%
Real Estate / Property / Construction	4	14,00%	14,00%	10,00%	10,00%
Retail	5	16,00%	15,00%	11,00%	11,00%
Telecommunications	2	11,00%	8,00%	6,00%	7,00%
Tourism & Hospitality	3	10,00%	11,00%	8,00%	8,00%
Transportation / Aviation / Aerospace	4	15,00%	14,00%	10,00%	10,00%
Utilities	2	8,00%	8,00%	6,00%	6,00%

Tableau 45-Ratios de réplication X1

E codes R

```
> model_weibull <- fitdist( ABC_table[weighted_dist<rho, Alpha] , 'weibull')
> model_weibull
Fitting of the distribution ' weibull ' by maximum likelihood
Parameters:
       estimate  Std. Error
shape 8.6524267 0.296000306
scale 0.2608128 0.001422217
> plot(model_weibull)
> ks.test(unique(ABC_table[weighted_dist<rho, Alpha]), 'pweibull', shape=model_weibull$estimate[1], scale=model_weibull$estimate[2])

 One-sample Kolmogorov-Smirnov test

data:  unique(ABC_table[weighted_dist < rho, Alpha])
D = 0.035617, p-value = 0.55
alternative hypothesis: two-sided
```

Figure 61 - Estimation d'une loi de Weibull