Mémoire présenté le :

pour l'obtention du Diplôme Universitaire d'actuariat de l'ISFA et l'admission à l'Institut des Actuaires

Par : Geoffrey Bard

Titre : Modélisation de la propagation d'un rançongiciel s'auto-diffusant

Confidentialité : ▫ NON OUI ☒ (Durée : ▫ 1 an ☒ 2 ans)
Les signataires s'engagent à respecter la confidentialité indiquée ci-dessus

Entreprise :
Nom : ADDACTIS FRANCE

Cachet :

Directeur de mémoire en entreprise :
Nom : Thomas Bastard

Signature : Thomas BASTARD

Membres présents du jury de l'Institut des Actuaires

D. Vallée

Invité :

Nom :

Signature :

Membres présents du jury de l'ISFA

P. Ribereau

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

Signature du responsable entreprise

Thomas BASTARD

Signature du candidat

Remerciements

Je remercie ...

— Thomas BASTARD, mon tuteur d'entreprise, pour ses nombreuses relectures, ses conseils, son sens de l'organisation et sa disponibilité tout au long de mon parcours au sein d'Addactis France,

— toute la Practice *Modeling & Risk* au sein du pôle *PnC* pour leurs idées et leur écoute, et en particulier Benjamin POUDRET pour l'opportunité qu'il m'a offerte à Addactis France,

— Pierre-Olivier Goffard, mon tuteur académique, pour ses nombreux conseils et ses idées qui ont enrichis le contenue de ce mémoire.

— mes très chers parents pour leur soutien sans faille, l'éducation qu'ils m'ont offerte, leur amour inébranlable,

— ma conjointe pour sa présence quotidienne et ses relectures nocturnes.

Résumé

Un rançongiciel est un logiciel malveillant chiffrant l'entièreté des données d'un dispositif informatique et réclamant le paiement d'une rançon afin de récupérer les données chiffrées. Certains de ces rançongiciels ont la capacité de s'auto-diffuser. C'est le cas de *Wannacry* et *NotPetya*, qui ont contaminé des milliers d'ordinateurs.

Le cœur de ce mémoire réside dans la modélisation de la propagation de ce type de rançongiciel, afin de mieux comprendre leur diffusion au sein d'un portefeuille d'entreprises assurées.

Après une succincte présentation du risque Cyber et des réglementations assurantielles liées à ce risque, un descriptif précis du fonctionnement des rançongiciels accompagné d'exemples est présenté. Le lecteur aura donc une meilleure représentation des enjeux et de ce risque si particulier.

Des rappels mathématiques concernant les modèles épidémiologiques, tels que le modèle SIR simple et multi-groupes et la théorie des graphes sont détaillés afin de mieux comprendre le fonctionnement de la propagation d'un rançongiciel s'auto-diffusant.

Introduit par le modèle collectif classique en assurance non vie, un modèle spécifique à ce risque est approfondi dans la suite de ce mémoire. Les impacts sur un portefeuille d'assuré, les différents coûts qu'un tel évènement peut engendrer et une modélisation du comportement des entreprises viennent compléter ce modèle. Un outil basé sur la théorie des graphes et les spectres laplaciens permettant de réduire le risque de propagation est également proposé.

Ensuite, une étude complète des bases de données Cyber, des crypto-monnaies et de statistiques est suggérée sur le segment des rançongiciels. Elle permet de mieux appréhender ce risque et constitue une première approche en termes de calibration des modèles.

Enfin, la justification de la calibration des paramètres des modèles est proposée, permettant d'appliquer la propagation d'un rançongiciel sévissant dans le monde entier. Ce scénario catastrophique fera également office d'une application de réassurance.

Mots-clés : *Ransomware*, *Rançongiciel*, PRC, VERIS, VCDB, *Cyber*, *Malware*, *Modèle épidémiologique*, SIR, SIS, *SIR Multi-groupes*, *Théorie des graphes*, *Spectre laplacien*, *Cyber-assurances*, *Bitcoin*, *Données à caractère personnel*

Abstract

Ransomware is malicious software that encrypts the entire data of a computer device and demands payment of a ransom to recover the encrypted data. Some ransomware has the ability to self-distribute. This is the case of *Wannacry* and *NotPetya*, which have infected thousands of computers.

The core of this master thesis lies in modeling the propagation of this kind of ransomware, in order to better understand their diffusion within a portfolio of insured companies.

After a brief presentation of the Cyber risk, and the insurance regulations related to this risk, a precise description of the functioning of ransomware is presented with examples. The reader will thus have a better representation of the stakes and of this very particular risk.

Mathematical reminders of epidemiological models, such as the simple and multi-group SIR model, and graph theory are detailed in order to better understand how the propagation of a self-diffusing ransomware works.

Introduced by the classic collective model in non-life insurance, a specific model for this risk is developed in the rest of this thesis. The impacts on a portfolio of insureds, the different costs that such an event can generate, and a modelling of the behaviour of companies complete this model. A tool based on graph theory and Laplacian spectra to reduce the propagation risk is also proposed.

Next, a complete study of Cyber, crypto-currency and statistical databases is proposed on the ransomware segment. It provides a better understanding of this risk, and constitutes a first approach in terms of model calibration.

Finally, the justification of the calibration of the models' parameters is proposed, allowing to apply the spread of a ransomware raging in the whole world. This catastrophic scenario will also serve as a reinsurance application.

Key-Words : *Ransomware*, PRC, VERIS, VCDB, *Cyber*, *Malware*, *Epidemiological model*, SIR, SIS, *SIR Multi-groups*, *Graph theory*, *Laplacian spectra*, *Cyber insurance*, *Bitcoin*, *Personal records*

Sommaire

Introduction

140 milliards d'euros : c'est le coût estimé en 2021 des pertes financières mondiale liées à l'arrêt d'activité des entreprises ou des services, consécutif à une attaque par rançongiciel selon une étude de la multinationale britannique *AON*. Ce nouveau risque Cyber, qui consiste à chiffrer les données d'un système informatique et à demander une rançon pour les récupérer, constitue un enjeu majeur des années à venir pour les entités assurantielles à deux niveaux : les rançongiciels ciblés qui ne visent qu'une seule entreprise et les rançongiciels s'auto-diffusant qui peuvent se propager aussi rapidement qu'un virus biologique. Dans le cadre du deuxième type de rançongiciel, la contamination de nombreuses entreprises demeure un risque qu'un assureur se tient d'appréhender et de maîtriser. Suite aux attaques massives de *Wannacry* et *NotPetya*, deux types de rançongiciel auto-répliquant, une attaque mondiale et sans précédent est un scénario qui a vu son statut évoluer de fictif à probable.

Telle est la question : comment et de quelle manière est-il possible de proposer une modélisation actuarielle de la propagation des rançongiciels s'auto-propageant en considérant les différents impacts et coûts auxquels un assureur doit faire face ?

Afin de mieux cerner l'émergence de ce risque, il est nécessaire de définir le risque Cyber dans sa généralité, ainsi que les conséquences auxquelles les assureurs s'exposent. La place du risque Cyber au sein de la norme Solvabilité 2 paraît également un point essentiel à intégrer. Enfin, le phénomène de propagation de ces rançongiciels nécessite un éclaircissement du fonctionnement de ces logiciels malveillants afin de justifier la modélisation de diffusion.

La première analogie la plus souvent émise est celle avec le monde biologique. En effet, la similarité entre les rançongiciels et les virus s'est renforcée au cours des années avec l'utilisation des modèles épidémiologiques classiques. Les règles, les taux de transmission et de guérison, ainsi que le modèle de compartiment définissant la diffusion probable d'un virus peut facilement s'étendre à la propagation du sujet de ce mémoire. Les processus de vaccination et de gestes barrières sont également des éléments assimilables au monde informatique avec la conception d'antivirus et la formation des employés à la Cyber-sécurité. C'est donc dans ce cadre-là, qu'il est nécessaire de déterminer les impacts et les coûts de ce nouveau risque. Ils ne sont pas que financiers, puisque l'assureur accompagne ses assurés à travers la crise, avec des entreprises de Cyber-sécurité, des cabinets d'avocats et même des juristes. Ainsi, si trop d'entreprises sont simultanément contaminées, l'assureur ne se doit pas d'être submergé par le nombre de ces assurés infectés. En d'autres termes, l'élimination de la crise par cette assistance est une composante du coût total et si l'assureur n'a pas la capacité de fournir cette aide, cela peut conduire à une augmentation drastique du coût des sinistres.

L'utilisation des graphes accompagnée d'un modèle Markovien dynamique temporel peut permettre à un assureur de mieux appréhender ses assurés les plus dangereux en termes de contamination. Les outils de théorie algébrique linéaire des graphes permettent de formuler un problème de demande d'assurance optimale. Grâce à l'analyse spectrale des matrices d'un graphe, il est possible de définir le degré de connexion des assurés entre eux, permettant de mieux cerner les causes du risque étudié. En

effet certains assurés peuvent être plus enclin à contribuer vivement à la propagation du rancongiciel. Si l'assureur est capable de les déterminer avant l'épidémie, alors il peut renforcer les mesures de prévention et intervenir en priorité lors d'une crise afin de réduire la diffusion du virus.

Cependant , la principale limite de l'étude du risque Cyber (et notamment le risque d'attaque par rançongiciel) est son manque cruel de données et d'historique. C'est dans cette dynamique qu'une étude de deux bases de données est proposée. Elle permet également de mieux saisir les enjeux de ce risque et de la réalité de ce phénomène. Un complément sur les crypto-monnaies et un sondage de *Sophos* viennent enrichir l'analyse des incidents dus à un rançongiciel.

Pour terminer, l'évaluation des paramètres d'un scénario catastrophique demeure une étape nécessaire pour un assureur. L'estimation des impacts qu'un tel scénario peut provoquer sur différents portefeuilles d'assurés permet de mieux cerner le risque. Le coût d'une telle catastrophe nécessite l'utilisation de la réassurance pour protéger la cédante. Une application liée à un traité XS est donc proposée.

Chapitre 1

Présentation du risque Cyber et mise en contexte

1.1 Cyber-attaques et Cyber-assurance

Selon le baromètre de la Fédération Française de l'Assurance, en 2021, le risque de Cyber-attaques se hisse en tête des risques émergents pour la quatrième année consécutive. La cartographie émise par la FFA met autant en garde sur la probabilité de survenance d'une Cyber-attaque que sur l'impact et les répercussions qu'un tel évènement peut engendrer. Au regard des statistiques alarmantes sur l'évolution des attaques informatiques depuis la crise épidémique du Covid-19, la Cyber-assurance demeure un enjeu incontournable des années à venir pour les acteurs de l'assurance.

Couvrant tous les risques de nature informatique, la Cyber-assurance amène à éclaircir la notion de risque de Cyber-sécurité, également appelé risque Cyber. Au sens de l'assureur, il est défini comme une affectation d'un élément appartenant au parc informatique d'un assuré, provoqué par une attaque malveillante ou une défaillance accidentelle. La notion de parc informatique réunit toutes les cibles propices aux Cyber-attaques : ordinateurs, serveurs, réseaux, appareils connectés, périphériques connectés, etc... Dans cette section, une définition et une classification des attaques dites malveillantes sont proposées. Dans un second temps, les garanties proposées par les assureurs, ainsi que les divers coûts engendrés seront étudiés. De prime abord il semble que ces pertes ne soient que financières ; en réalité elles sont plus diversifiées qu'il n'y paraît.

1.1.1 Cyber-attaques : Définition et classification

En raison de son hétérogénéité, le terme *Cyber-attaque* demande à être approfondi. C'est pourquoi le gouvernement français propose une classification des types de risque Cyber pour une entreprise. Ainsi, le site de l'État soumet quatre familles quelle que soit la cible affectée :

— la Cyber-criminalité,
— l'atteinte à l'image,
— l'espionnage,
— le sabotage.

Sans doute la famille la mieux connue du grand public, la Cyber-criminalité centralise toutes les attaques ayant pour objectif de récupérer des informations à caractère personnel. Les types d'attaque

restent cependant variés puisque l'objectif consiste à accéder aux informations protégées. Une fois obtenues, les Cyber-criminels cherchent généralement à exploiter ces données ou/et à les revendre. À contrario de la croyance générale, les cibles sont également diversifiées puisque leur taille coïncide souvent avec le niveau de Cyber-sécurité du parc informatique, mais n'est pas corrélé avec la sensibilité des données. Ainsi, une petite ou moyenne entreprise (PME) ayant une activité de e-commerce peut détenir des données personnelles propres à sa clientèle (données bancaires, adresse électronique, mot de passe, ect...). Les institutions publiques et les grandes entreprises détiennent quand à elles des données personnelles souvent en quantités massives même si plus difficiles à obtenir.

L'atteinte à l'image s'apparente généralement à des revendications politiques, économiques et même idéologiques. Ici, l'intention est de bloquer l'accès à un site informatique ou de modifier le contenu de ce dernier. Le type d'attaque propre à ce genre de déstabilisation est l'attaque par déni de service, qui sera détaillé dans la liste des différentes attaques existantes.

L'espionnage est également un enjeu crucial du 21ème siècle. Utilisé à des fins économiques, industrielles et scientifiques, ce type de Cyber-attaque nécessite une préparation minutieuse. Le profil des Cyber-criminels est ordinairement un groupe organisé, ciblant précisément leur victime et agissant avec dextérité. Une attaque peut être amenée à durer plusieurs années. Il est difficile pour une entreprise de s'apercevoir qu'elle en est victime. En effet, les attaques utilisées sont le plus souvent imperceptibles puisqu'il n'y a pas de programme qui s'exécute en surface. Les utilisateurs sont donc persuadés de ne pas être infectés.

Enfin, le sabotage tend à rendre inutilisable un système informatique. L'exemple le plus connu concerne sans doute les hôpitaux, qui sont massivement victimes de virus, ayant pour objectif d'affecter totalement les systèmes hospitaliers, privant l'hôpital d'informations cruciales sur ses patients. Ces informations deviennent "monnayables" et une rançon est exigée afin d'y accéder.

Ces 4 familles généralisent donc les types de Cyber-attaques que peut subir une entité. Cependant, il reste à définir les piratages du point de vue informatique. Il sera appelé "attaque informatique", tout acte malveillant envers un dispositif informatique. Même si la motivation du mémoire demeure les rançongiciels, il a semblé pertinent de spécifier les différentes attaques car la présentation du risque Cyber ne se contraint pas qu'au rançongiciel et que certaines attaques interviennent dans le processus des rançongiciels.

1.1.1.1 Attaque par déni de Service

Comme évoqué précédemment, *Distributed Denial of Service attack* (DDOS) ou attaque par déni de Service distribué en français, a pour but de saturer temporairement un service via l'inondation de la bande passante par plusieurs machines en simultané. Un Cyber-criminel va donc surcharger plusieurs requêtes au même instant sur un serveur. Même si une information de connexion (i.e. un ping) contient par défaut 32 octets, il est possible d'allouer jusqu'à 65 527 octets. En multipliant ce nombre de ping, il est rapidement possible d'inonder le service et de le rendre inaccessible ou gravement ralenti pendant la durée de l'attaque. En réalité, les Cyber-criminels ont recours à des structures informatiques permettant d'envoyer un volume important d'octets par seconde. À titre d'exemple, la plus grande attaque par DDOS en France envoyait 265 gigabits par seconde, ce qui représente 33,13 gigaoctets par seconde (puisque 1 octet contient 8 bits). Avec cette quantité d'information, le service attaqué sature et ne peut plus fonctionner correctement.

En termes de statistique, le volume d'attaques par DDOS en nombre est de 83 600 en France en 2020 selon *International Featured Standard* (ITR). Une augmentation de 128 % a été observée par rapport à l'année précédente. La pandémie de la Covid-19 est sans doute responsable de cette évolution

puisque la mise en place du télétravail a favorisé ce genre de pratique, car les connexions particulières étant bien plus faciles à saturer que des serveurs professionnels.

1.1.1.2 Les *malwares*

Les *malwares* regroupent tous les logiciels malveillants. Il existe une multitude de programmes nuisibles s'installant sur un système informatique sans demander préalablement le consentement de l'utilisateur. Ces attaques ne sont pas forcément ciblées et apparaissent à la suite d'une mauvaise manipulation de la victime ou une vulnérabilité du système d'exploitation. Cette catégorie d'attaque est subdivisée en trois classes selon Wikipédia :

— mécanisme de propagation : propagation via réseau, faille du système d'exploitation, clé USB
— mécanisme de déclenchement : le *malware* apparaît à la venue d'un évènement . Le nombre de redémarrage du disque dur est par exemple un évènement . (On parle alors de bombe logique)
— charge utile : suppression de fichier nécessaire au fonctionnement de l'ordinateur, rendant un démarrage impossible.

Enfin certains de ces *malwares* sont des virus informatiques et ont la capacité de s'autorépliquer, c'est à dire de se propager sans intervention humaine à d'autres machines utilisant le réseau comme voie de transmission. Les rançongiciels appartiennent à la famille des *malwares* puisqu'il s'agit d'un logiciel malveillant composé d'un script visant à chiffrer l'entièreté des données du disque dur. Son fonctionnement sera détaillé plus tard. Il sera noté également dans cette catégorie, des noms répandus comme les chevaux de Troie, les vers informatiques, ou encore les *spywares* (logiciel espion). Une baisse du nombre d'attaques des *malwares* a été signalée l'année dernière passant de 10,5 milliards en 2018 à 5,6 milliards en 2020. Cependant cette statistique n'est pas représentative du danger des rançongiciels. En effet, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) a estimé que les incidents dus à ce type de *malware* ont triplé en France en 2020 par rapport à 2019. Autre statistique alarmante, celle du nombre de tentatives d'attaques par rançongiciel. En 2019, la fréquence était estimée à une attaque toutes les 14 secondes contre 11 en 2021.

1.1.1.3 Ingénierie Sociale, brute-force et dictionnaire

Ce sont les attaques les plus faciles à mettre en place, elles sont utilisées pour trouver des mots de passes, des données bancaires ou encore pour faciliter l'installation d'un *malware* sur une machine. L'ingénierie sociale dont l'attaque la plus répandue est le *phishing* (hameçonnage) consiste à exploiter les faiblesses psychologiques des victimes, autrement dit des failles humaines et non informatiques. Pour illustrer ce propos, le fonctionnement du *phishing* est le suivant : on recopie à l'identique un service, comme un mail ou un site informatique, puis on demande à l'utilisateur de saisir des données sensibles comme son mot de passe. L'utilisateur peut donc croire que cette demande est réelle et fait donc confiance à la provenance de ce service. Une fois saisie, la donnée sensible est directement récupérée par le Cyber-criminel lui permettant de jouir de son gain. Il faut savoir que sur le darknet, une quantité invraisemblable de mails, de mots de passe associés et de données bancaires circulent et se revendent à prix d'or. De plus, l'obtention de ce genre de données permet la mise en place d'autres attaques, mais l'ingénierie sociale n'est pas le seul moyen d'obtenir facilement ce type d'informations.

Sans doute, une des plus anciennes attaques, la méthode par force brute consiste à tester, l'une après l'autre, chaque combinaison possible de caractère dans le but d'obtenir un mot de passe. Rapidement limité par le nombre de caractères, cette technique permet en général de tester des petites combinaisons. En effet, l'ajout d'un caractère dans un mot de passe rend le temps d'exécution exponentiellement bien plus long. La capacité de tester des combinaisons par seconde dépend de la puissance du CPU

(processeur) ou du GPU (carte graphique). Il est estimé aujourd'hui qu'avec des modèles de GPU (Gtx 1060) datant de 2017, il est possible de tester 3,9 millions possibilités par seconde, tandis qu'un modèle actuel (RTX 3090) permet d'obtenir 669 millions tests par seconde. Ainsi, l'évolution des GPU caractérisée par la puissance de calcul demandée par des jeux-vidéos ou des logiciels de modélisation 3D vont permettre à certains Cyber-criminels d'employer à nouveau cette méthode. Similairement, il existe le dictionnaire qui consiste à tester les mots les plus courants. Ainsi, on peut trouver sur internet des bases de données comportant tous les mots d'une langue. À l'aide d'un algorithme, il est donc possible de tester tous les éléments de cette base de données. Le seul moyen développé à ce jour pour contrer ce genre d'attaque demeure la double authentification : quand une nouvelle connexion est établie depuis une adresse *Internet Protocol* (IP) inconnue par le serveur, une authentification par mail ou téléphone est demandée à l'utilisateur. Le Cyber-criminel n'ayant pas accès à cet outil, sa connexion est impossible.

1.1.2 Contrat d'assurance : risques couverts et garanties

Les contrats d'assurance couvrant le risque Cyber se sont multipliés ces récentes années. Considérés comme une protection supplémentaire, ces nouvelles garanties tendent à se normaliser dans les entreprises. Les récentes attaques ont poussé les compagnies à la souscription d'une police de Cyber-assurance. Néanmoins, le rapport Hiscox 2020 sur la gestion du risque Cyber signalent que seulement 23% des entreprises déclarent s'être assurées contre ce risque.

En effet les contrats responsabilité civile professionnelle et/ou dommage (comme à titre d'exemple la tout risque informatique) ne couvrent pas explicitement les risques Cyber. Même si toute police qui ne comporte pas une exclusion explicite (i.e. police silencieuse) peut être exposée, plusieurs risques encourus à la suite d'une Cyber-attaque ne sont pas des polices explicites, tels que :

— pertes de données à caractère personnel (DCP) de l'entreprise et de tiers,
— frais de nettoyage des systèmes,
— perte d'exploitation,
— frais de notification aux tiers concernés,
— assistance auprès d'autorités compétentes,
— sanctions prononcées par une autorité administrative,
— gestion de crise.

Chaque contrat d'assurance dédié au risque Cyber est différent. Les garanties ainsi que les exclusions de garanties ne sont pas normalisées. Naturellement les primes demandées évoluent selon les clauses du contrat. Cependant, 3 volets de protection sont généralement présents dans les garanties. De plus, la nature des garanties va permettre d'établir la modélisation des risques et des coûts auxquels les assureurs peuvent faire face dans le risque Cyber.

La première différence présente dans les contrats d'assurance Cyber est l'origine de l'attaque subie par l'assuré. Pourtant, 3 origines dissemblables pouvant altérer les garanties peuvent être distinguées :

— l'erreur humaine : l'attaque est rendue possible par une action involontaire d'un salarié. L'ouverture d'un mail infecté en est un exemple,
— une brèche technique : l'attaque se propage à l'entreprise par le biais d'un incident technique, ou d'une faille inconnue,
— les dénis de service : il n'y a pas de responsable, ni de brèche technique ; c'est le système informatique qui est surchargé.

1.1.2.1 Volet 1 : assistance à la gestion de crise

Dans l'optique d'accompagner ses assurés à la suite d'une Cyber-attaque, les compagnies d'assurance offrent dans ce volet des garanties d'assistance technique en collaboration avec la direction d'entreprise. L'objectif de ce volet est d'une part de soulager l'assuré et d'autre part de contenir la propagation de l'attaque et les répercussions médiatiques. Les assureurs en association avec des experts spécialisés proposent généralement les garanties suivantes :

- mise à disposition de consultants juridiques en cas de procès, d'experts en communication pour limiter l'impact de l'atteinte à l'e-réputation et de spécialistes en Cyber-sécurité afin que l'assuré soit de nouveau autonome,
- téléassistance toujours ouverte pour prévenir de la crise,
- négociation avec les Cyber-criminels.

1.1.2.2 Volet 2 : Cyber-dommages et pertes financières

Ces garanties dédommagent les pertes financières subies par l'entreprise à hauteur d'un plafond préalablement défini. En effet ces conséquences pécuniaires peuvent s'avérer exorbitantes. Ainsi l'assureur souhaite soutenir la stabilité de l'activité économique de l'entreprise à la suite de la crise. La police d'assurance contient ce type de garanties, même si certaines peuvent être des garanties exclues :

- perte d'exploitation,
- paiement de la rançon (de plus en plus exclu),
- indemnisation des frais juridiques, informatiques et de communication,
- le coût du remplacement du parc informatique endommagé.

1.1.2.3 Volet 3 : responsabilité civile

Pouvant rapidement passer du statut de victime à celui de responsable, les assureurs s'engagent à endosser les dommages qui peuvent être subis par les collaborateurs, les clients ou encore les partenaires de l'entreprise. On retrouve donc une responsabilité civile en cas de mise en cause par des tiers (collaborateurs) ou par les autorités administratives.

1.1.2.4 Exclusions de garanties et clauses ambiguës

Comme pour tous contrats classiques de l'assurance, la prime sera relative aux nombres de garanties exclues. La Cyber-assurance étant encore à ses prémices, les différents assureurs contractualisent des exclusions propres à leur jugement. Tandis que certains stipulent que les dommages matériels ne sont pas indemnisés après une Cyber-attaque, d'autres refusent le paiement de la rançon. Cette dernière exclusion semble se généraliser par une volonté politique commune puisque le Sénat, l'ANSSI (Agence nationale de sécurité des systèmes informatiques) et le parquet de Paris ont récemment critiqué les assureurs remboursant ce paiement. Enfin, l'erreur humaine peut également faire jouer des clauses ambiguës dans le contrat.

Après l'attaque NotPetya, le géant de l'agro-alimentaire Mondelez a assigné en justice son assureur Zurich qui a refusé toutes indemnisations en stipulant que ce rançongiciel était "un acte de guerre Russe" et que ce risque là n'était pas couvert dans le contrat. La Russie ayant nié toute responsabilité dans cette Cyber-attaque, le procès semble bien engagé pour Mondelez.

1.2 Solvabilité 2 et le risque Cyber

L'objectif de cette section est de rappeler les points fondamentaux de la directive Solvabilité 2, de comprendre la place du risque Cyber dans cette directive afin d'introduire les applications à l'assurance du dernier chapitre. On essayera de proposer l'intégration de ce risque dans les modèles internes à la différence des modèles formule standard. L'ORSA sera également évoqué, l'outil d'analyse décisionnelle de Solvabilité 2, permettant de cerner les éléments de nature à modifier la solvabilité des assureurs.

1.2.1 Solvabilité 2 : rappel et fonctionnement

Imaginée par l'Union Européenne en 2009 et légiférée en 2016, Solvabilité 2 est une directive européenne dans la continuité de Solvabilité 1, qui consiste à soumettre tous les organismes assureurs (i.e. assureurs, mutuelles, réassureurs...) européens à la même régleme ntation en termes de fonds propres. En effet, le fonctionnement d'un organisme d'assurance est différent de celui des entités économiques. Son cycle de production étant inversé, ce dernier ne peut pas connaître la somme qu'il va verser à ses clients. Par analogie, une entreprise classique connaîtrait le prix auquel elle achète ses matières premières seulement après avoir vendu son stock. Il existe donc pour ces organismes un risque de solvabilité, autrement dit, un risque de ne pas pouvoir faire face à ces engagements auprès de ses clients (assurés) sur le long terme. Au regard de cette menace, Solvabilité 2 contraint donc les assureurs à calculer, à mesurer ce risque et exige sa communication auprès du grand public. Cette décomposition d'étapes se traduit par l'existence de trois piliers reflétant chacun une volonté particulière de la directive.

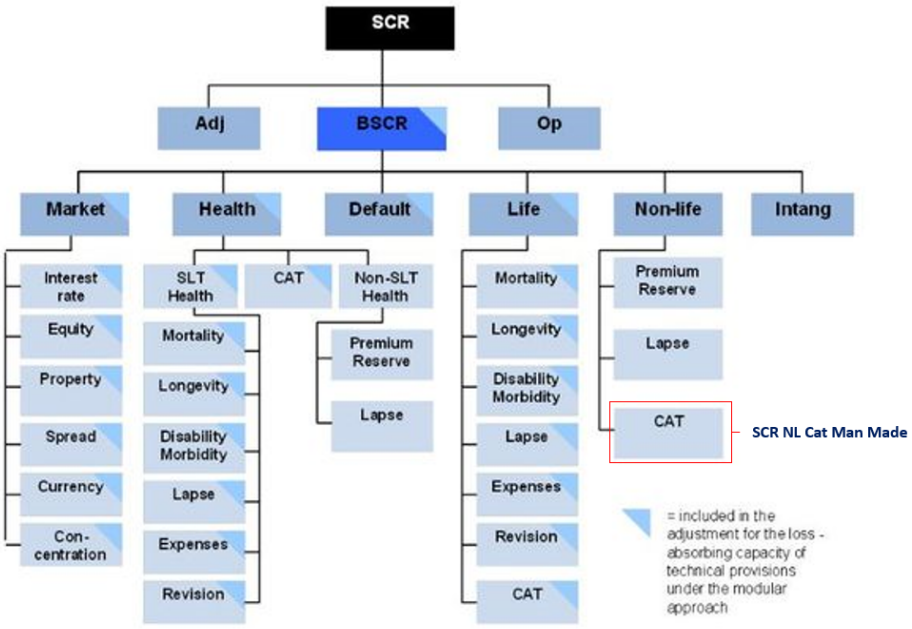

FIGURE 1.1 – Rappel de la décomposition du SCR, ainsi que le sous-groupe auquel le risque Cyber doit appartenir.

1.2.1.1 Pilier 1 : exigences quantitatives

Le premier pilier intègre des exigences liées directement aux fonds propres. Il impose des normes quantitatives de calculs permettant aux entités d'assurances de mesurer le risque de solvabilité.

- le **Minimum Capital Requirement** (MCR) symbolise le seuil minimum de fonds propres nécessaires. Il permet aux institutions de contrôle de veiller à ce que tous les organismes détiennent un capital économique suffisant à son bon fonctionnement. C'est un calcul standardisé par le pilier,
- le **Solvency Capital Requirement** (SCR) est basé sur une formule standardisé qui a pour but de garantir que chaque organisme puisse faire face à tous les risques quantifiables. Le SCR est décomposé en plusieurs sous SCR selon les branches d'activités. Une matrice de corrélation des risques permet de calculer le SCR global.

À noter qu'il existe en réalité deux approches de calcul. La première approche est fournie par les autorités de régulation européennes. Les assureurs appliquant ces calculs standardisés répondent alors à la formule standard. Dans un second cas, il est possible de développer sa propre approche en justifiant son fonctionnement auprès des autorités compétentes. Ces assureurs ne sont alors plus en formule standard, mais en modèle interne.

1.2.1.2 Pilier 2 : exigences qualitatives

Le pilier 2 indique les enseignements nécessaires aux entités assurantielles en termes d'organisation. Plus communément appelés exigences qualitatives, ce pilier définit les points essentiels de gouvernance et de décisions à mener afin de garantir un pilotage réfléchi face au risque de solvabilité. Le régulateur peut également imposer un capital supplémentaire si nécessaire.

Toujours dans le cadre de la gestion des risques, le pilier 2 a implémenté l'idée d'une hiérarchie organisationnelle comprenant quatre fonctions clés nécessaires à ces exigences qualitatives.

- fonction de gestion des risques,
- fonction audit interne,
- fonction de vérification de la conformité,
- fonction actuariat.

Enfin ce pilier contient l'ORSA (Évaluation interne des risques et de la solvabilité - *Own Risk and Solvency Assessment*). Ce processus d'analyse décisionnelle permet de lier les exigences quantitatives aux exigences qualitatives. Les trois évaluations obligatoires soumises par l'ORSA sont :

- le besoin global de solvabilité (BGS),
- la couverture permanente des besoins de couverture de solvabilité,
- l'écart entre le profil de risque de l'entreprise et les hypothèses de la formule standard.

1.2.1.3 Pilier 3 : exigences de communication

Solvabilité 2 exige la transparence totale des assureurs vis-à-vis des 2 premiers piliers. C'est ainsi que le pilier 3 s'inscrit dans une communication harmonisée auprès des autorités de contrôle, comme l'ACPR (Autorité de Contrôle Prudentiel et de Résolution), ou encore du grand public. Le pilier 3 soumet donc les assureurs à :

- une transmission minutieuse et conciliante des normes quantitatifs (MCR, SCR, bilan prudentiel) par des *reportings* au niveau européen,

— une diffusion transparente et harmonisée de l'information financière via des QRT (*Quantitative Report Template*),
— la vigilance à la qualité des données afin de ne pas accroître le risque opérationnel.

1.2.2 Gestion du risque Cyber dans Solvabilité 2

Défini comme un risque d'origine humaine (i.e. risque *Man-Made*), le risque Cyber ne dispose pas de son propre module dans la formule standard, à la différence de certains modèles internes. Néanmoins, la formule standard tente de prendre en compte le risque Cyber dans les calculs des modules du SCR non-vie suivants :

— *SCR non-vie primes et réserves* : simule la sous-tarification des contrats Cyber ou le sous-provisionnement des sinistres Cyber,
— *SCR non vie cessation* : simuler le choc de la cessation d'une partie des contrats Cyber,
— *SCR Other* : simule un choc sur 40% de la prime Cyber,
— *SCR non-vie CAT* : dans des modèles internes, utilisation du $99,5^{\text{ème}}$ percentile de la courbe de distribution obtenue pour la couverture à protéfer dans la captive.

De plus, dans un objectif d'harmonisation, le pilier 3 exige une refonte en profondeur des QRT (*Quantitative Reporting Templates*) ou la production de nouveaux QRT permettant de mettre en évidence le risque Cyber.

1.3 Rançongiciel : histoire et fonctionnement

1.3.1 Première apparition

Selon Wikipédia, il faut remonter en 1989 pour retrouver la première forme de rançongiciel créé par un biologiste américain. À cette époque, le virus de l'immunodéfience humaine (VIH) a été découvert quelques années auparavant et sa connaissance du grand public demeure encore faible. C'est ainsi que le Docteur Joseph Popp envoya par voie postale une disquette appelée *AIDS Information Introductory Diskette* dans plusieurs pays afin d'informer le public du danger de ce virus. Derrière le contenu informatif se cachait une bombe logique qui provoquait après 90 démarrages de l'ordinateur un chiffrement de l'entièreté des données du disque dur et faisait apparaître un message de demande de rançon s'élevant à 189 dollars. Le paiement devait se faire à une entreprise domiciliée au Panama. Cependant, le créateur du premier rançongiciel n'avait prévu que le chiffrement du nom des fichiers et non pas leur contenu, rendant directement son *malware* inoffensif. Arrêté par Scotland Yard qui retrouva sa piste par le biais de sa compagnie, il est extradé aux États-Unis où il sera déclaré mentalement inapte à être jugé. De plus, la loi américaine montra un vide juridique face à ces pratiques. Il affirmera aussi que l'argent récolté devait servir à la recherche contre le VIH.

L'histoire du rançongiciel aurait pu s'arrêter ici, mais l'exposition médiatique du biologiste poussera Adam Young et Moti Yung à publier *Cryptovirology : Extorsion-Based Security Threats and Countermeasures*, un ouvrage traçant l'ensemble des étapes nécessaires à la création d'un rançongiciel.

1.3.2 Définition et fonctionnement : de Young & Yung à la pratique

1.3.2.1 Proposition d'une définition

Comme soutenu plus haut, un rançongiciel, ou *ransomware* en anglais, est un logiciel malveillant appartenant à la famille des *malwares*. Après s'être glissé dans un système informatique via généralement le réseau, le rançongiciel chiffre discrètement l'entièreté des données des disques durs. Une fois cette étape terminée, un message s'affiche, informant du chiffrement et exigeant une rançon qui une fois payée permet d'accéder à la clé de chiffrement. Le paiement se fait actuellement par le biais des cryptomonnaies (e.g. *Bitcoin*), puisqu'il est quasiment impossible de connaître l'identité de la personne se cachant derrière une adresse d'une cryptodevise. La rançon s'élève à quelques centaines d'euros et à tendance à varier selon le cours des cryptoactifs.

Les rançongiciels sont constamment confondus avec les *wipers*. Ces derniers appartiennent également à la famille des *malwares* et leur fonctionnement est similaire, à défaut que les données ne sont pas récupérables. Il arrive parfois qu'une rançon soit demandée mais une fois que la victime s'en est acquittée, les données restent chiffrées.

Enfin, il est nécessaire de différencier deux types de rançongiciels :
— les rançongiciels auto-répliquant : capable de se diffuser rapidement via un mode de transmission défini, correspondant généralement au réseau,
— les rançongiciels ciblés : les Cyber-criminels ont déterminé leur cible et ne se concentre que sur la diffusion du rançongiciel au sein de l'entreprise.

À noter que l'on parle de déchiffrer quand une clé de décodage existe et de "*décrypter*" quand ce n'est pas le cas.

Cette courte définition amène à pousser la compréhension globale du fonctionnement de ce genre de *malware*. En reprenant la publication de Young & Yung, une définition limpide sera établie.

1.3.2.2 Programmation et chiffrement

Souvent caché dans un type de fichier innocent, le rançongiciel n'est qu'un simple script dont la programmation peut être effectuée depuis de nombreux langages de programmation. Les quelques fonctions du script ont pour objectif de :
— lister l'ensemble des disques durs de la machine,
— lister l'ensemble des dossiers de chaque disque dur,
— lister l'ensemble des fichiers de chaque dossier,
— chiffrer l'ensemble des fichiers avec une clé unique par machine,
— supprimer tous les fichiers non chiffrés,
— afficher la demande de rançon.

Dans l'étude de Young & Yung, les deux chercheurs montrent que le recours au chiffrement asymétrique demeure un choix idéal. Pour rappel, le chiffrement symétrique correspond à utiliser des clés identiques pour chiffrer et déchiffrer. Ainsi cette option est plus rapide, mais est facilement déchiffrable par une analyse statique ou dynamique. A contrario, le chiffrement asymétrique génère une clé de chiffrement, appelée clé publique et une clé de déchiffrement, appelée clé privée. Ainsi, chaque machine infectée possède une paire de clés uniques (publique et privée). Il faudra tout de même attendre 2005, soit 16 ans après *AIDS* pour que les Cyber-criminels appliquent les consignes de Young & Yung.

1.3.2.3 Gestion des clés, des fichiers et du paiement

Comme stipulé par les deux experts du chiffrement, la gestion des clés reste délicate par sa méthode mais également par le recours à un serveur C2 (serveur de commande et de contrôle). Après infection de la machine, le rançongiciel idéal se doit d'envoyer un ping (i.e. un paquet de données) au serveur

C2, qui génère les deux clés uniques. En retour, le serveur C2 transmet au rançongiciel la clé publique pour chiffrer les données, mais conserve la clé privée afin d'éviter qu'elle soit contenue dans la machine infectée. Cependant, de nombreux *proxy*, pare-feu, ou réseaux peuvent bloquer la communication entre le *malware* et le serveur. Dans la pratique, certains rançongiciels embarquent directement une clé publique générée aléatoirement par le binaire du *malware*. En cas de problème de connexion avec le serveur C2, seule la clé privée n'est pas générée, mais le chiffrement a quand même lieu. Cependant, le déchiffrement n'étant pas possible, la rançon devenait inutile. Ainsi, le seul bémol auxquels Young & Yung n'ont pas su répondre est le problème de connexion.

En ce qui concerne la gestion des fichiers, il existe deux alternatives de chiffrement :
- le *malware* ouvre les fichiers en mode lecture et écriture (Accès au contenu et modification possible), puis chiffre le fichier en modifiant l'extension. Les fichiers ne sont pas réellement supprimés, mais seulement modifiés,
- les fichiers sont seulement ouverts en mode lecture et une copie chiffrée est effectuée par le *malware*, avant d'effacer l'original. La suppression nécessite un balayage complet des disques durs. En effet, une simple suppression d'un fichier n'efface pas son contenu, mais seulement son inode (i.e. sa structure de données, comme son nom, sa taille, son emplacement etc..).

Pour la gestion du paiement, les groupes de Cyber-criminels s'étaient orientés vers les paradis fiscaux en utilisant des sociétés écrans. Cependant, elles étaient facilement traçables par les services de l'ordre. Les hackers se sont donc dirigés vers des moyens de paiement plus simples comme *UKash* ou *Paysafe-Card*. Ces derniers nécessitaient un processus de blanchiment long , ouvrant des brèches plus nombreuses aux enquêteurs. L'apparition du *Bitcoin* en 2009 réjouit donc les Cyber-criminels, puisque les transactions demeurent quasiment intraçables et anonymes. C'est ainsi que 98% des rançongiciels l'utilisent. Certaines transactions datant d'avant 2018 ont fructifié au regarder de l'évolution du cours du *Bitcoin*. Même s'il est extrêmement complexe de remonter une transaction, des organismes comme le FBI ont déjà réussi ce défi.

1.3.2.4 Principe de la Cyber Kill Chain

Développé par des informaticiens de la société *Lockheed Martin*, la Cyber Kill Chain est une modélisation du processus d'une Cyber-attaque. Elle est adaptable au processus d'attaque d'un rançongiciel. L'objectif est donc de proposer les différentes étapes auxquelles les groupes Cyber-criminels font face. Contrairement à des idées reçues, le processus d'attaque pour un rançongiciel peut durer plusieurs mois. Cette modélisation est divisée en 7 étapes.
- reconnaissance,
- armement,
- distribution,
- exploitation,
- installation,
- commande & contrôle,
- action finale.

La reconnaissance : le but primordial de cette étape est de cibler sa victime en collectant un maximum d'informations. C'est donc ici qu'interviennent des attaques en force brute ou par *phishing*. En accédant à ses données, le Cyber-criminel peut s'assurer du poste, de la qualité des données et des communications de la victime. Deux approches victimologiques restent à déterminer afin de mieux comprendre la réflexion des auteurs pour cibler les attaques :
- selon le secteur d'activités des entreprises,
- selon la zone géographique.

L'armement : le mot armement désigne la technique utilisée par le *malware* pour se camoufler en fichier inoffensif. Il existe des méthodes classiques dont l'utilisation d'extensions multiples ne résistant pas aux antivirus, ainsi que différents langages de scripts, ou même des failles du système d'exploitation.

La distribution : cette étape consiste à transmettre le rançongiciel par un moyen de communication. La messagerie électronique demeure la voie la plus utilisée. Cela s'explique par le fait que les utilisateurs sont plus dubitatifs à la réception d'un mail personnel que professionnel. Ainsi, les mails dans le monde professionnel sont une des branches de distribution la plus fréquente.

L'exploitation : l'ingénierie sociale ou piratage psychologique est le principal moyen de déclencher une action de l'utilisateur. Les fourberies utilisées par les pirates ne manquent pas de créativité. Internet regorge de pièges et il est souvent difficile de faire le tri. À noter que cette étape n'est pas nécessaire au rançongiciel s'autorépliquant.

L'installation : le *malware* s'assure qu'il soit dans des conditions idéales pour arriver à son objectif. La première phase est d'obtenir les privilèges d'administrateur afin d'effacer les *Shadow Copy* (i.e. technologie permettant les sauvegardes de fichiers) et de rechercher les serveurs critiques stockant les identifiants. Enfin les portes dérobées sont de plus en plus courantes, car elles permettent d'observer les activités du réseau et de mieux cerner les failles essentielles.

La commande et le contrôle : ce sont les moyens de communication entre la machine infectée et le serveur C2. Il est possible d'y ajouter le mouvement latéral, consistant pour un rançongiciel à intégrer le chiffrement des données externes comme une clé USB ou encore des sauvegardes dites cloud. De plus en plus de *malwares* s'attardent sur ces mouvements afin d'être le plus efficace possible et de forcer au paiement de la rançon.

L'action finale : l'étape ultime est généralement la rançon. La présence d'un compte à rebours sur le message demandant la rançon permet de stresser l'utilisateur pour un paiement plus rapide. Cependant l'action finale peut également être une Cyber-attaque de sabotage, dans le cas d'un *wiper*.

1.3.3 Divers faits marquants

1.3.3.1 WannaCry

Arrivé en mai 2017, *WannaCry* est sans doute le rançongiciel le plus connu à ce jour. Premier rançongiciel à se propager automatiquement, il aurait infecté plus de 300 000 machines dans plus de 150 pays. Afin de mieux comprendre cette capacité à s'autopropager, il semble pertinent d'expliquer son moyen de transmission. Le 14 avril 2017, l'Agence Nationale de la sécurité (NSA) a révélé et publié deux failles du système d'exploitation Windows. La première se nomme *EternalBlue* et est une exploitation d'une vulnérabilité dans le protocole *Server Message Block (SMB)* qui permet le partage des ressources dans un réseau local, autrement dit, permet de prendre le contrôle d'une machine à distance et d'y infiltrer son virus. La seconde est *DoublePulsar*, une porte dérobée permettant à l'assaillant d'avoir la permission de surveiller la machine infectée et d'exécuter des commandes et l'installation du rançongiciel.

Alertée par ces failles, l'entreprise de *Microsoft* a de suite proposé une mise à jour bloquant la possibilité d'utiliser ces deux codes offensifs. Cependant, de nombreux utilisateurs n'ont pas pris le temps de réaliser ces *updates*. C'est ainsi que les Cyber-criminels à l'origine de *WannaCry* ont recyclé les deux codes de la *NSA* et les ont couplés à un rançongiciel. Ce cocktail informatique a donné naissance à un *malware* capable de s'autodiffuser. Apparaissant en Espagne et au Royaume-Uni, il aura suffi de moins de 48 heures pour infecter plus de 100 000 systèmes Windows. La *National Health*

Service estimera les dommages causés par le virus à plus de 100 millions de dollars. On notera parmi ses victimes la présence de *Renault*, *Le ministère de l'intérieur russe* et de *FedEx*

En termes d'innovations, *WannaCry* demeure comme une réelle prouesse technique pour ce qui est de la propagation, mais semble contenir de grandes lacunes sur l'axe rançongiciel sûrement en raison de la volonté des hackers d'attaquer le plus rapidement les utilisateurs n'ayant pas fait la mise à jour. On peut donc supposer qu'une meilleure préparation de rançongiciel aurait causée des dommages bien plus désastreux pour les entreprises.

1.3.4 NotPetya

Il faudra attendre seulement 1 mois après *WannaCry* pour observer un nouveau *malware* (*wiper*). En juin 2017, c'est *NotPetya*, dont le nom provient de *Petya* un ancien *malware* de 2016, qui frappe les entreprises ukrainiennes. Utilisant similairement les mêmes failles que *WannaCry*, il se fait passer pour un logiciel de comptabilité. Touchant l'Ukraine en premier, il se propage au reste du monde et s'attaquera également à des grands groupes comme *Mars*, *Nivea*, la centrale nucléaire de Tchernobyl ou encore l'entreprise française *Saint-Gobain*. À titre d'exemple, c'est tout le réseau de distribution de la société française qui est suspendu, entraînant une perte majeure de données nécessaires au fonctionnement du géant français. On estimera la perte à 220 millions d'euros, représentant 0,5% du chiffre d'affaires annuel. Le coût total du *wiper* est évalué entre 1 et 10 milliards de dollars. La largeur de cet intervalle s'explique d'une part, par le manque d'informations cruciales sur le nombre d'entreprises infectées refusant de communiquer pour éviter la décrédibilisation de son image marketing et la chute de son action ; et d'autre part aussi par la difficulté à estimer le coût d'une donnée. Il faut noter que *NotPetya* n'est pas à proprement parler un rançongiciel, mais un *wiper*. Ainsi aucune clé de déchiffrement n'existe et son objectif n'était pas l'argent mais le sabotage et la destruction de données informatiques.

1.3.5 *Ransomware As A Service* (RAAS) & Colonial Pipeline

La compagnie pétrolière *Colonial Pipeline* exploite le plus grand oléoduc des États-Unis et alimente plus de 45% des livraisons sur la côte est. Le 6 mai 2021 l'entreprise est victime d'une Cyber-attaque de type rançongiciel, chiffrant l'entièreté de leur parc informatique. Paralysée par ce *malware*, elle est obligée de cesser tous ses activités pendant une courte durée, notamment à cause de l'inaptitude à utiliser son logiciel de facturation. L'information circulant rapidement sur le nouveau continent, une pénurie d'essence éclate provoquant une panique générale des citoyens allant jusqu'à faire des réserves personnelles d'essence. Le groupe *DarkSide*, à priori basé en russie, a également réussi à dérober des données personnelles et confidentielles de l'entreprise.

Cet exemple permet d'illustrer dans un premier temps l'intensité qu'une Cyber-attaque peut avoir sur l'économie d'un pays, mais aussi le modèle économique du groupe Russe. En effet, ils ont utilisé un service bien connu des criminels informatiques, le *Ransomware As A Service (RAAS)*. Ce service illégal propose le développement et l'exécution d'un rançongiciel contre une partie du gain obtenu. De plus en plus prisé par les Cyber-terroristes, le RAAS va même jusqu'à négocier les rançons avec les victimes. Enfin des affiliés peuvent être recrutés par les groupes malveillants sur des plateformes comme le darknet afin de s'occuper de la partie diffusion et propagation du *malware*. Par exemple, certains affiliés vont développer des vers informatiques incluant l'installation d'un rançongiciel créé par une tierce personne à chaque nouvelle machine infectée. On peut même notifier que le service client de *DarkSide* a transmis une faible partie des fichiers déchiffrés à *Colonial Pipeline* afin de justifier l'existence de la clé de déchiffrement.

Au regard des conséquences sociétales aux États-Unis, les professionnels de *DarkSide* ont publié un message affirmant qu'ils se désolidarisaient de cette attaque en justifiant que leur objectif était seulement économique et n'avaient nullement l'objet de créer des problèmes sociétaux. Cette soudaine rédemption a surtout pour but d'éviter que toutes les infrastructures américaines se mettent à la recherche des hackers en tentant de remonter les transactions. S'il avait été réellement sincère, le groupe aurait pu simplement fournir la clé de déchiffrement. Au lieu de ça, une entente entre les deux parties a été trouvé et une rançon de plusieurs millions d'euros a été effectuée (s'élevant à 75 *Bitcoin*). Même si ce chiffre peut paraître exorbitant, il demeure bien moins élevé que le coût de la perte d'exploitation de la société pétrolière. C'est ainsi que le directeur général de *Colonial Pipeline*, *Joseph Blount* a déclaré "J'admets que je n'étais pas à l'aise avec le fait de voir de l'argent s'évaporer et aller vers de telle personne, mais c'était la bonne chose à faire pour le pays "

Pour information, la crainte de *DarkSide* était bien fondée, puisque les services secrets américains ont réussi à remonter les paiements du *Bitcoin* et à récupérer plus de 60 *Bitcoin* sur les 75 payés. Toutefois, avec la chute du cours de la cryptomonnaie, la somme récupérée s'avérait plus faible que la valeur de base.

Chapitre 2

Approche d'une modélisation de propagation

L'objectif de ce chapitre est de présenter mathématiquement un type de modèle approchant au mieux la propagation d'un rançongiciel s'auto-diffusant. De nombreux travaux existent et proposent des modèles différents. La motivation du choix du modèle de ce mémoire sera justifiée après la présentation des différentes modélisations existantes. Cette liste n'est pas exhaustive.

2.1 Les différentes modélisations de propagation actuelles

Les différentes littératures s'attaquant à la modélisation de la diffusion d'un *malware* utilisent fréquemment une des modélisations suivantes.

2.1.1 Processus de *Hawkes*

Par définition, les processus ponctuels représentent des évolutions stochastiques d'une variable aléatoire. Ces processus se divisent en plusieurs familles et les processus de *Hawkes* en forment une. Imaginé dans les années 70 par A.G Hawkes, ces processus aléatoires peuvent modéliser la répartition de points dans l'espace et le temps. Ils sont caractérisés par l'auto-excitation. En effet, un processus de *Hawkes* est un processus de Poisson dont l'intensité n'est pas constante (dans la majorité des cas), mais dépendante du temps. Ce phénomène de processus auto-excitant permet une modélisation de "réaction en chaîne". Ainsi, plus l'intensité du processus est importante, plus la probabilité qu'elle soit élevée augmente. En d'autres termes, la survenance d'un évènement entraîne une augmentation de la probabilité qu'un autre évènement survienne rapidement.

Les domaines d'application de ces processus de comptage sont donc généralement des phénomènes caractérisés par la survenance d'évènements déterministe. L'utilisation d'origine fût la modélisation des séismes. En effet, la singularité de l'auto-excitation de ces processus permet de mieux simuler les répliques engendrées par un premier tremblement de terre. Les domaines d'application peuvent s'élargir également à la neuroscience, aux réseaux sociaux ou à la finance statistique (notamment aux conséquences qu'une première faillite peut avoir). Enfin les phénomènes d'excitation et de dépendance

dans le risque Cyber sont également modélisables par des processus ponctuels comme *Y.Bessy-Roland* [4] l'illustre dans son mémoire s'intitulant "*Modélisation stochastique individuelle de sinistres Cyber*". Par ailleurs, les paramètres calibrant les processus de Hawkes (i.e. λ_0, α et β) sont également définis dans ce papier.

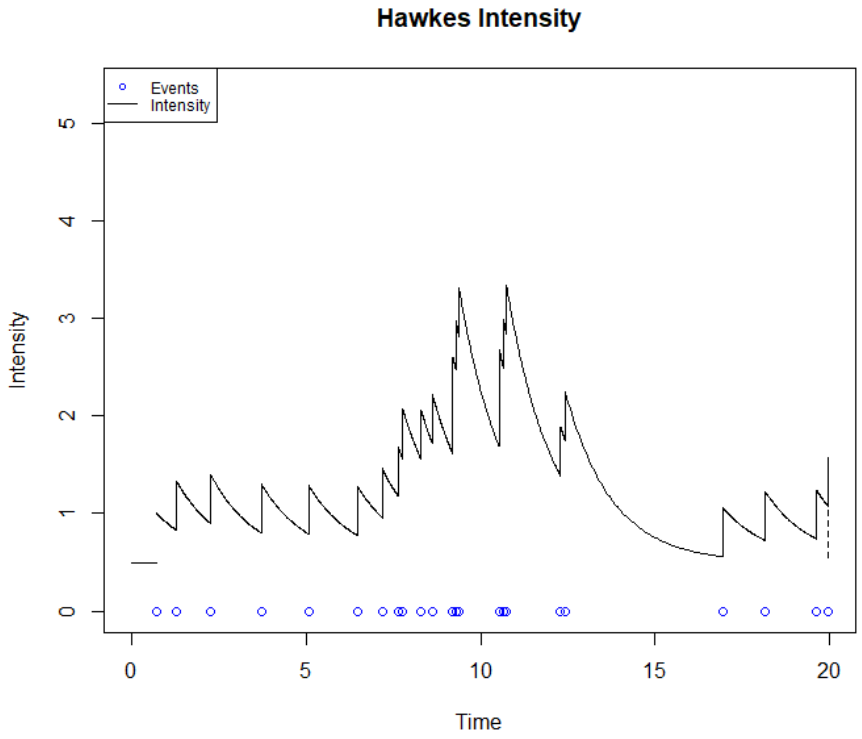

FIGURE 2.1 – Exemple de l'intensité d'un processus de Hawkes avec $\lambda_0 = 0,5$, $\alpha = 0,5$ et $\beta = 0,75$

Dans le domaine de la propagation, les processus de Hawkes sont pertinents. Ils permettent entre autres d'obtenir des informations cruciales sur les diverses corrélations entre les "assurés". Cependant, le paramétrage des processus de Hawkes nécessitent un minimum d'informations et de données sur le sujet à modéliser. À la vue du manque de données et d'historique du risque de rançongiciel s'auto-diffusant, l'utilisation des processus de Hawkes semble délicate.

2.1.2 Système multi-agents

Les systèmes multi-agents (SMA) sont une branche de l'informatique permettant la modélisation de situations ardues liées généralement à des problématiques sociétales. Ces SMA peuvent être représentés par un monde virtuel où tous les éléments le régissant sont préalablement définis dans l'algorithme. Ces éléments peuvent se diviser en plusieurs catégories :

— un environnement,
— des agents,
— des objets,
— des interactions et ensemble d'opérateurs.

Afin de mieux assimiler la définition des éléments cités, un exemple de simulation de la propagation du choléra de la ville de Ngaoundéré au Cameroun présent dans *"Modélisation et simulation multi-*

agent de la propagation d'une épidémie de choléra : cas de la ville de Ngaoundéré" par *G. Kolaye, E. Mbuge, J-C.Kamgang* et *S. Bowong* [10] servira d'analogie.

La ville de Ngaoundéré, divisée en plusieurs zones, correspond à l'environnement du SMA. Ainsi, il dispose d'une métrique et régit l'espace de vie des agents. Ces derniers correspondent à la population susceptible d'être infecté par le choléra. Par définition, les agents sont les intermédiaires qui possèdent la faculté d'interagir entre eux et avec le reste des éléments. Cette population interagit avec des lieux de leur quotidien, comme les marchés, les écoles, ou encore les entreprises. Ces objets (ici, les lieux) sont donc inertes mais permettent la création d'une interaction spécifique entre l'agent et eux. Les fonctions régissant les actions des agents sont donc les interactions. Par exemple, le fait de communiquer avec un autre agent est une interaction parmi tant d'autres. En se rendant à un emplacement spécifique, l'individu réalisera une action précise qui sera définie par l'ensemble d'opérateurs.

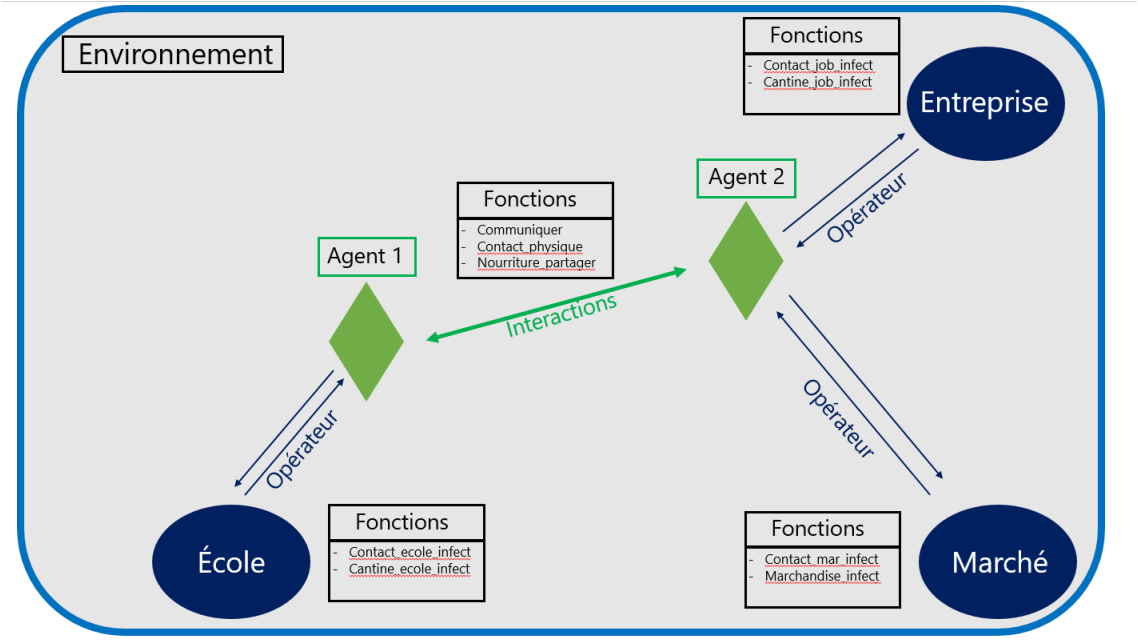

FIGURE 2.2 – Exemple simplifié du SMA modélisant la propagation du choléra.

Pour résumer, le SMA est un programme simulant un monde virtuel où les interactions sont au cœur de l'algorithme. Comme évoqué dans l'exemple du choléra, la propagation d'une épidémie peut être modélisé par des SMA. De multiples travaux traitent des domaines plus ou moins connexes tels que la création d'un service de VTC, les réseaux, la modélisation cognitive ou encore les comportements des êtres vivants.

Cependant, à la vue de la pauvreté des données Cyber et de son historique, un modèle aussi précis semble compliqué à mettre en œuvre. De plus, cette modélisation nécessite une forte expertise des langages de programmation orientée objet. Enfin, la complexité de ces algorithmes entraîne généralement des exécutions informatiques de plusieurs jours. Ainsi, il a été préférable de s'orienter vers d'autres modélisations qui a priori répondaient mieux aux critères évoqués ci-dessus.

2.1.3 Modèles compartimentaux

Les modèles compartimentaux demeurent un outil pertinent pour décrire la propagation des différentes maladies infectieuses. À la vue des nombreuses littératures abordant cette thématique, de l'adaptabilité des modèles et de l'analogie entre les virus biologiques et informatiques, le choix du modèle utilisé dans le mémoire se basera largement sur ce type de modélisation. Leurs fonctionnements et la justification de ce choix sont abordés dans la section suivante.

2.1.4 Théorie des graphes et spectre laplacien

L'histoire raconte que *Leonhard Euler* visita la ville de Königsberg en 1735. L'ancienne capitale de la Prusse se structure autour de 7 ponts permettant d'accéder à deux îles et de traverser son fleuve. *Euler* constitua à partir de cette structure un problème de topologie : est-il possible de visiter la ville en empruntant une seule fois chaque pont pour n'importe quel point de départ ?

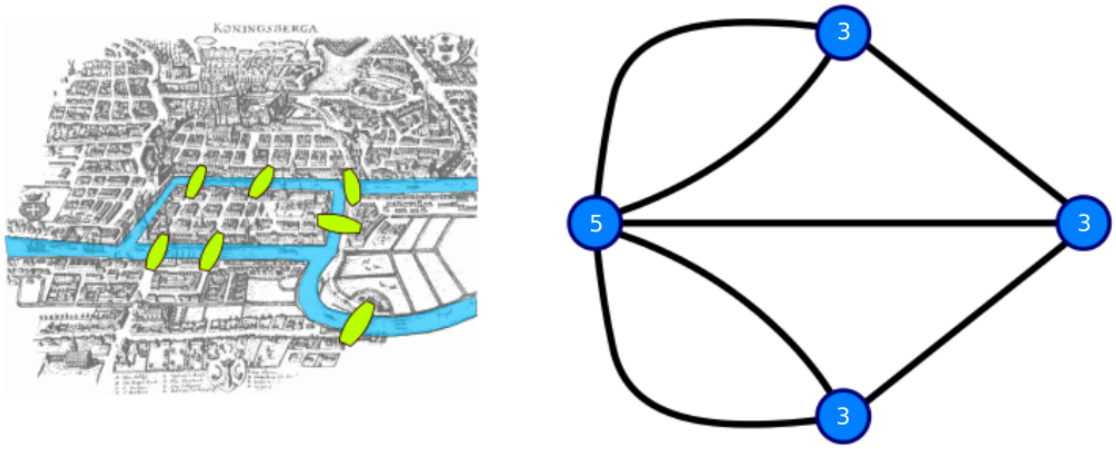

FIGURE 2.3 – Structure de la ville de Königsberg et transformation en graphe

La réponse à ce problème demeure triviale et même si la démonstration n'a pas réellement un intérêt mathématique, il demeure comme la naissance de la théorie des graphes. En effet, *Euler* démontra qu'en décomposant la structure de la ville en graphe, où les sommets représentent les zones séparées par le fleuve et les arêtes correspondent aux ponts, il s'avère que, quel que soit le point de départ, il est impossible de passer une seule fois par chaque pont.

Ainsi, la théorie des graphes est apparue et donnera naissance à une nouvelle branche des mathématiques permettant d'étudier la structure de différents réseaux. Des outils mathématiques ont été développés donnant des informations sur la connexion globale des graphes (spectre laplacien), le plus court chemin, ou encore sur des points de passages importants . Cette théorie est désormais utilisée dans de nombreux domaines comme la structure des réseaux sociaux, informatiques ou encore la génétique.

2.2 Les modèles compartimentaux simples en épidémiologie

2.2.1 Histoire, motivation et fonctionnement

Repris en 1927 par Anderson Gray McKendrick et William Ogilvy Kermack et améliorés quelques années plus tard, les modèles compartimentaux sont des approches de modélisation dédiées aux maladies infectieuses. Réintroduits dans les années 1980 avec le SIDA et ces dernières années avec la crise sanitaire de la Covid-19, cet outil épidémiologique demeure une approximation fondamentale de la propagation des virus. Néanmoins, les maladies infectieuses ont bien souvent des caractéristiques uniques (transmission, mortalité, symptômes, durée, etc...). L'adaptation des modèles demeure donc flexible. Ainsi, il existe une multitude d'extensions cherchant à correspondre à certaines infections particulières.

La construction d'un scénario de rançongiciel se propageant automatiquement semble modélisable via les modèles compartimentaux. En effet, une analogie entre les maladies infectieuses et les rançongiciels, ainsi qu'entre les individus et les entreprises peut se constater. Dans le cadre d'une maladie infectieuse, chaque individu de la population observée est attribué à un compartiment du modèle, selon son état face à l'objet biologique. Il est ainsi possible d'attribuer les mêmes caractéristiques aux entreprises, qui par leur communication peuvent se transmettre le *malware*. L'objectif demeure donc de simuler la propagation du *malware*. De plus, l'analogie peut également s'établir sur les spécificités de certaines actions prises en compte dans les modèles. Un parallèle entre un vaccin et des mises à jour du système d'exploitation, entre des mesures sanitaires et la formation des employés à la Cyber-sécurité, ou un confinement à l'isolation des communications entre les entreprises semble opportun. C'est ainsi que le choix de ces modèles pour appuyer la démarche de propagation et de diffusion du rançongiciel se justifie.

Comme brièvement expliqué, la composante principale des modèles compartimentaux est la population concernée par le danger. Dans le cas du rançongiciel, la population peut être définie par des machines ou des entreprises. Comme le nom l'indique, l'approche de cette modélisation associe à chaque individu de la population un compartiment en fonction de son état. Si l'individu contracte le rançongiciel, ou si ce n'est pas encore le cas, le compartiment de ce dernier ne sera pas le même. Ces modèles peuvent donc permettre de régir la dynamique de la diffusion du *malware*. À chaque instant de l'épidémie, il est possible de comprendre et d'analyser sa propagation selon la proportion d'individu présente dans les compartiments via des paramètres caractérisant la diffusion.

Le fonctionnement précis du modèle varie selon le nombre et le type de compartiments. Pour rappel, ces modèles ont été pensés selon les caractéristiques des maladies infectieuses et selon la population étudiée. Il semble donc pertinent de les présenter et de justifier leur efficacité à représenter au mieux la propagation d'un rançongiciel.

Les trois caractéristiques principales de ces modèles sont donc les compartiments, leurs règles et le temps. On désigne par N, avec $N \geqslant 2$, la population totale sensible à l'épidémie. La somme des individus présents dans les compartiments est donc égale à N quel que soit t, le temps passé après la constatation de l'attaque. Le nombre d'individus présents dans les compartiments à l'instant t est donc symbolisé par :

- $S(t)$ avec $S(t) \leqslant N$ où S, pour *susceptible*, désigne les individus exposés à la maladie mais toujours sains pour le moment. Ce compartiment est présent dans tous les modèles proposés dans cette section,
- $I(t)$ avec $I(t) \leqslant N$ et $I(0) > 0$ où I, pour *infected*, contient tous les individus ayant contractés la maladie. On supposera donc que ces individus peuvent transmettre la maladie au reste de la population. Ce compartiment est également nécessaire à chaque modélisation étudiée,
- $E(t)$ avec $E(t) \leqslant N$ où E, pour *exposed*, englobe les individus qui ont contracté le virus, mais ne peuvent pas la transmettre. Cela illustre dans le monde biologique, le temps de latence entre la contraction de la maladie et la capacité à contaminer les autres individus,
- $R(t)$ avec $R(t) \leqslant N$ où R, pour *removed* indique les individus guéris et ayant une immunité contre la maladie. Dans la réalité biologique, ce compartiment est représenté par les personnes

guéries, ainsi que décédées. Puisque dans le cadre des rançongiciels, il s'agit de machines informatiques, les décès ne seront pas utilisés. Le terme *removed* correspondra uniquement à la notion de guérison pour plus de simplicité.

Certains modèles prennent en compte d'autres compartiments, comme le décès, la vaccination, la quarantaine et également le taux de natalité et le taux de mortalité. Cependant, à la vue de la modélisation désirée, les éléments cités ne seront pas abordés dans ce mémoire.

L'évolution des individus dans chaque compartiment, autrement dit le passage d'un compartiment à un autre, est régie par des règles. Trois taux interviennent donc dans ces règles et sont nécessaires au fonctionnement du modèle :

— β avec $\beta > 0$ équivaut au taux de transmission. β permet donc de représenter le taux de personnes susceptibles qui deviennent infectées,
— γ avec $\gamma > 0$ équivaut au taux de guérison, c'est à dire le taux de personnes infectées qui n'appartiennent plus à cet état à instant t. Plus ce taux est élevé, plus la guérison est courte. Ainsi $\frac{1}{\gamma}$ représente la durée pendant laquelle une personne est contagieuse,
— α avec $\alpha > 0$ équivaut au taux d'incubation. La durée d'incubation est donc le temps de latence entre la contraction et la contagion de la maladie.

Notons, S (resp. I, E et R) la fonction du compartiment des individus *susceptibles* (resp. *infected*, *exposed* et *removed*), tel que t avec $t \in [0, T]$ où T est le temps de la fin de l'épidémie. On a :

$$\begin{array}{rccc} S & : & [0,T] & \to & [\![0,N]\!] \\ & & t & \mapsto & S(t) \end{array}$$

où $S(t)$ (resp. $I(t)$, $E(t)$ et $R(t)$) représente le nombre d'individus dans S à l'instant t.

Notons C_1 et C_2, deux fonctions définies comme précédemment, où la population est répartie entre ces deux compartiments et a et b deux taux positifs régissant ce modèle épidémiologique.

On peut affirmer qu'à l'instant t

$$C_1(t+dt) = C_1(t) - aC_1(t)dt + bC_2(t)dt$$

$$\Leftrightarrow C_1(t+dt) - C_1(t) = -aC_1(t)dt + bC_2(t)dt$$

$$\Leftrightarrow \frac{dC_1(t)}{dt} = -aC_1(t) + bC_2(t)$$

On obtient donc une équation différentielle permettant de connaître le nombre d'individus à un instant $t + dt$. La variation de la fonction $C_1(t)$ est donc donnée par le signe de sa dérivée. Il est donc possible de décrire l'évolution au cours du temps de la population dans les différents compartiments.

2.2.2 Les différents modèles existants

2.2.2.1 Le modèle SI (*susceptible*, *infected*)

Au début du $XX^{\text{ème}}$ siècle, une violente peste frappe la ville de *Bombay*. Dans un objectif de modélisation, William Heaton Hamer imagine le modèle SI en 1906. L'hypothèse faite par le médecin suppose qu'un individu infecté le reste à vie. Néanmoins, malgré son fort taux de mortalité, il est tout à fait possible d'en guérir. Cette omission fait par Hamer engendra une modélisation complètement faussée. Ce modèle convient donc à des maladies transmissibles et incurables.

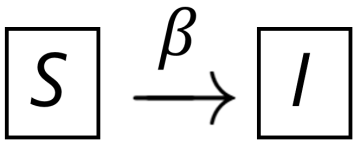

FIGURE 2.4 – Schéma des compartiments du modèle SI

Ce modèle est composé de deux compartiments, S pour *susceptible* et I pour *infected* Un seul paramètre est utilisé dans cette modélisation. C'est le β représentant le taux de transmission. Les équations différentielles régissant ce modèle à l'instant t sont :

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta S(t)I(t) \end{cases}$$

L'adaptation de ce modèle dans le cadre d'un rançongiciel est impertinent. Les entreprises infectées ne le seront pas définitivement et le fait de payer une rançon ou d'accepter la perte de données permet de sortir du compartiment I. Il est donc nécessaire d'ajouter un autre compartiment.

2.2.2.2 Le modèle SIS (*susceptible*, *infected*, *susceptible*)

Plus adapté aux maladies où la mutation est envisageable ou que l'immunité est inexistante, telle que la gastro-entérite ou la rhinopharyngite, le modèle suppose qu'après avoir guéri de la maladie, le sujet devient à nouveau exposé à l'épidémie. Ainsi, le modèle se divise en 2 compartiments (S pour *susceptible*, I pour *infected*). Cette modélisation est régie par 2 paramètres : β, le taux de transmission et γ le taux de guérison. Le modèle est décrit par les équations différentielles suivantes :

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t) + \gamma I(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta S(t)I(t) - \gamma I(t) \end{cases}$$

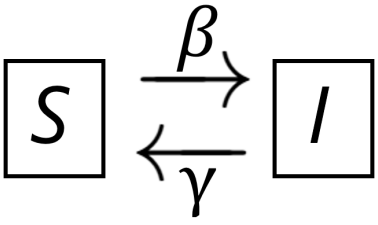

FIGURE 2.5 – Schéma des compartiments du modèle SIS

Dans le cas d'un rançongiciel, il semble judicieux de ne pas avoir ce retour au compartiment S possible. Une entreprise infectée sera premièrement bien plus consciente du risque Cyber et s'entourera d'entreprises spécialisées dans la Cyber-défense afin d'éviter tout nouveau risque. De plus, une sauvegarde des données sera effectuée en aval de l'attaque et il semblera bien plus difficile de perdre la totalité des informations cruciales dont dispose la compagnie. Cependant, ce modèle apporte une dimension intéressante au niveau de sa modélisation. Le fait de n'avoir que deux états permet d'utiliser

un modèle probabiliste simple comme une variable aléatoire de Bernoulli couplée à un processus de poisson.

2.2.2.3 Le modèle SIR (*susceptible*, *infected*, *removed*)

Réellement théorisé par Kermack et McKendrick pour des maladies généralement mortelles comme la peste noire, ou la grippe espagnole, le modèle SIR suppose que l'état d'un individu peut évoluer du compartiment *susceptible* à *infected* jusqu'à *removed*, où le dernier compartiment signifie soit l'immunité soit le décès. (Pour les rançongiciels, on ne parlera que d'immunité, autrement dit de guérison). Dans le cadre Ainsi, à la différence du modèle précédent, le retour au compartiment S n'est pas possible. Les deux taux caractérisant le modèle sont le taux de transmission β et le taux de guérison γ. Les équations différentielles représentant la modélisation sont donc les suivantes :

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta S(t)I(t) - \gamma I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) \end{cases}$$

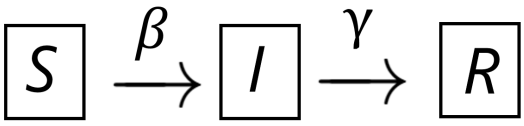

FIGURE 2.6 – Schéma des compartiments du modèle SIR

Plus adapté à des maladies existantes, ce modèle sert encore à modéliser la propagation de virus tel que la Covid-19. Par ailleurs, de nombreux travaux utilisent cette théorie dans la modélisation de la propagation de *malware*. Il semble plus pertinent par son hypothèse à retirer des individus sensibles à l'épidémie. De plus, certaines actions comme la vaccination peuvent être appliquées en supposant qu'une partie de la population appartient déjà au compartiment R.

2.2.2.4 Le modèle SEIR (*susceptible*, *exposed*, *infected*, *removed*)

Ce modèle est divisé en 4 compartiments (S pour *susceptible*, E pour *exposed*, I pour *infected* et R pour *removed*). Comme expliqué précédemment, ce modèle permet de mettre en évidence la latence de la contraction de la maladie. Il est supposé ici que la maladie devient transmissible à partir d'un certain moment. Ainsi, avant d'être infecté, un individu passera obligatoirement par le compartiment *exposed* où il ne sera pas dans la capacité de transmettre la maladie. Généralement, les personnes dites exposées n'ont pas conscience d'avoir contracté la maladie puisque les symptômes ne sont pas encore présents. Cela peut expliquer le temps nécessaire pour observer le résultat des mesures sanitaires et barrières mises en place lors de la crise sanitaire de la Covid-19.

Les différents taux du modèle sont toujours le taux de transmission β, le taux de guérison γ, mais également le taux d'incubation α qui modélise cet effet de latence. Les équations différentielles du modèle SEIR sont donc les suivantes :

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t) \\ \frac{\mathrm{d}E(t)}{\mathrm{d}t} = \beta S(t)I(t) - \alpha E(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \alpha E(t) - \gamma I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) \end{cases}$$

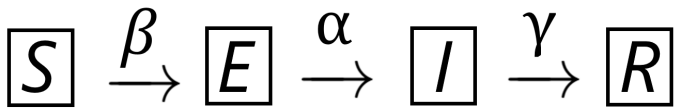

FIGURE 2.7 – Schéma des compartiments du modèle SEIR

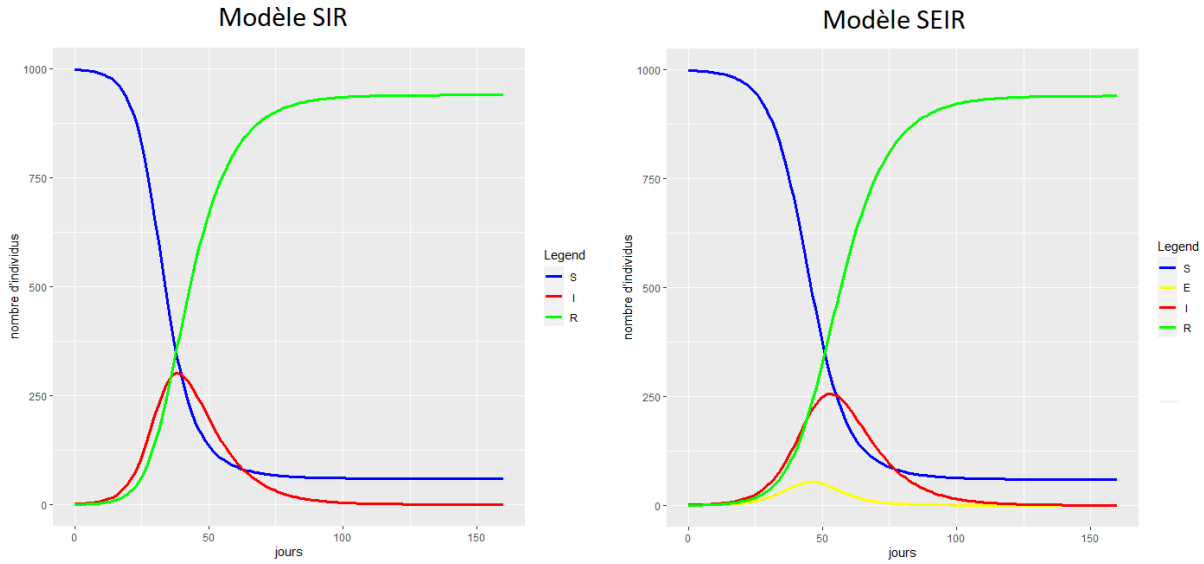

FIGURE 2.8 – Simulation du modèle SIR et SEIR avec les mêmes taux β et γ

2.2.3 Choix du modèle épidémiologique pour les rançongiciels

Parmi tous les modèles présentés dans la sous-section précédente, il est nécessaire de déterminer le modèle et les hypothèses qui correspondent au mieux à la modélisation de la propagation d'un rançongiciel. Dans le cadre d'un scénario de ce type de *malware*, on suppose que n'importe quel assuré du portefeuille de l'assureur est exposé au risque sous-jacent. Plusieurs éléments comme le secteur d'activités, la zone géographique ou encore les communications entre les assurés peuvent étendre la propagation de l'épidémie. Lors de l'attaque, le premier assuré touché sera donc infecté. Après un certain temps, cet assuré ne le sera plus. Deux hypothèses sont alors possibles : soit il peut encore subir l'attaque, soit il n'est plus exposé à ce risque. Il est difficile d'admettre la première hypothèse. En effet, après avoir été attaquée, l'entreprise corrigera les failles de son système de sécurité et stoppera son activité. Ainsi, on admet que l'assuré deviendra immunisé contre ce rançongiciel.

À la vue de la structure d'une attaque de rançongiciel et des éléments décrits précédemment, les modèles SI et SIS ne correspondent pas réellement aux caractéristiques propres de ce genre de *malware*,

alors que les modèles SIR et SEIR semblent plus adaptés grâce à la présence du compartiment R. Ces deux derniers se différencient par le pas de latence dû au compartiment E, visuellement justifié par la figure 2.5. L'analogie entre les maladies infectieuses et les rançongiciels reste plus délicate sur l'élément de l'incubation. Même si l'absence de la connaissance de l'infection est similaire, la période d'incubation peut largement varier selon le rançongiciel. Certains commencent le chiffrement à l'instant où le virus a infecté la machine, tandis que d'autres sont programmés pour agir après plusieurs démarrages. Dans le cadre des *malwares* s'auto-propageant, on suppose que le chiffrement est instantané, puisque la propagation est automatique. Ainsi, le choix du modèle SIR à la place du SEIR est donc plus cohérent avec cet éclairage.

En ce qui concerne le paramétrage du taux de transmission et du taux de guérison, le modèle SIR est déterministe, c'est à dire que le paramètre est fixé à l'avance et est connu avant que les résultats de la modélisation apparaissent. Il est tout à fait envisageable de transformer ce modèle déterministe en modèle stochastique. Dans ce cas les paramètres suivront une loi et seront déterminés par le résultat de cette loi. À la vue du manque de données et d'historique, le calibrage des paramètres demeurent impossibles. L'utilisation du registre du *Bitcoin* peut contribuer à une meilleure visualisation de ces paramètres (Cette méthode sera utilisée dans le chapitre suivant). Le choix du modèle déterministe ou stochastique sera justifié dans la suite du mémoire.

2.2.4 Analyse du modèle SIR

L'objectif de cette sous-partie est de présenter une analyse mathématique complète du modèle SIR afin de pouvoir directement intégrer les notions suivantes à l'analogie du rançongiciel, ainsi que dans le modèle SIR multi-groupes. Pour cela, il est nécessaire de définir les concepts subséquents.

2.2.4.1 Fonctionnement et concepts du modèle SIR

Proposition 1. *On note C une fonction de t avec $t \in [0, +\infty]$. On a donc :*

$$\begin{array}{rccc} C & : & [0,+\infty] & \to & [\![0,N]\!] \\ & & t & \mapsto & C(t) \end{array}$$

où $C(t)$ représente le nombre d'individus dans C à l'instant t.

Finalement cette fonction est associée aux différents compartiments du modèle SIR, dont la proportion d'individus évolue au cours du temps. L'évolution du nombre d'individus dans chaque compartiment est définie par le théorème suivant :

Théorème 1. Soit S, I et R, des compartiments du modèle SIR, β (avec $\beta > 0$) et γ (avec $\gamma > 0$) deux paramètres fixés, N avec $N > 2$ la taille de la population, t, avec $t > 0$ l'évolution du temps. On note que $S(0), I(0), R(0) \in [0, N]^3$ Le système d'équations différentielles suivant permet de décrire la dynamique du modèle SIR :

$$\begin{cases} \frac{\mathrm{d}S(t)}{\mathrm{d}t} = -\beta S(t)I(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} = \beta S(t)I(t) - \gamma I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} = \gamma I(t) \end{cases}$$

Ce système est non linéaire et ne propose pas de solution analytique.

Théorème 2. La population étudiée et exposée à la maladie est notée N quel que soit t avec $t \geqslant 0$ tel que

$$N = S(t) + I(t) + R(t)$$

Ce théorème découle du fait que la population totale est divisée dans les trois compartiments. Ainsi chaque individu est affecté à un état particulier à chaque instant de l'épidémie.

Définition 1. On définit s (resp i, r), le pourcentage d'individus présents dans le compartiment S (resp I, R), tel que $s = \frac{S}{N}$ (resp $i = \frac{I}{N}$, $r = \frac{R}{N}$). On obtient donc que $s + i + r = 1$.

Cette définition permet de plus facilement intégrer certaines notions. De plus, de nombreuses littératures utilisent directement ces notations.

2.2.4.2 Seuil épidémique : taux effectif de reproduction et taux basique de reproduction

L'épidémie de la Covid-19 a mis en lumière la notion de taux de reproduction dans le cadre d'une crise sanitaire. Pourtant, certaines définitions médiatiques ne correspondent pas à la réalité. C'est ainsi qu'il faut distinguer deux taux pourtant liés : *le taux basique de reproduction* R_0 et *le taux effectif de reproduction* R_e

Définition 2. *le taux basique de reproduction* R_0

On définit R_0, le taux basique de reproduction à $t = 0$, i.e. le nombre moyen de nouveaux infectés par un individu infectieux, tel que $R_0 = \frac{\beta}{\gamma}$. Ce taux permet donc de connaître au début d'une épidémie, la mesure de l'amplitude de propagation de l'agent pathogène.

Le R_0 peut être décomposé en plusieurs variables afin de mieux déterminer les facteurs propices à la propagation d'une maladie, tel que $R_0 = \frac{\beta}{\gamma} = D\kappa\tau$ avec $\beta = \kappa\tau$ et $\gamma = \frac{1}{D}$ où :

— D : La durée de l'infection,
— κ : le nombre de contacts d'un individu infecté avec des individus susceptibles,
— τ : la transmissibilité.

Le taux basique de reproduction est un indicateur clé des épidémies. Il sert à connaître à la vitesse de propagation et mesure l'aptitude de l'agent pathogène à se propager. Il peut varier d'une maladie infectieuse à l'autre, puisque le γ est propre à chaque maladie (le temps de guérison est différent selon l'infection) et que le taux de transmission est différent pour chaque infection. Si ce R_0 est supérieur à 1, le nombre d'individus infectés croîtra jusqu'à une certaine limite : soit toute la population est contaminée, soit le $R_e(t^*)$ est inférieur à 1 et l'épidémie décroît. Pour information, on estime le R_0 de la Covid-19 entre 2 et 3 tandis que celui de la rougeole est d'environ 15.

Définition 3. *le taux effectif de reproduction* R_e

On définit R_e, le taux effectif de reproduction à $t = 0$, la valeur seuil ou point de basculement qui détermine si une maladie infectieuse va rapidement s'éteindre ou si elle va envahir la population et provoquer une épidémie, tel que $R_e(0) = \frac{\beta S(0)}{\gamma N} = \frac{\beta s(0)}{\gamma}$. Ainsi, on définira que $\forall t > 0, R_e(t) = \frac{\beta s(t)}{\gamma}$

À noter que dans le cas général, on considère que $S(0) = N - 1$, c'est à dire qu'il existe une seule personne infectée. Ainsi, quand N est grand, on peut facilement admettre que $R_e(0)$ est proche du taux suivant :

$$R_e(0) = \frac{\beta}{\gamma} = R_0$$

2.2.4.3 Variations des fonctions et nombre maximum d'individus infectés

Les équations différentielles du modèle SIR telles que présentées permettent l'analyse du sens des variations des 3 fonctions (S, I, R) grâce au signe des dérivées. Ces variations complètent la compréhension du modèle SIR et permettent de mieux cerner la structure de la propagation d'une épidémie. Les fonctions S et R sont monotones et leur maximum est connu.

Proposition 2. *Variation des fonctions $S(t)$et $R(t)$*

- *β, $S(t)$, $I(t)$ sont positifs, donc $\frac{\mathrm{d}S(t)}{\mathrm{d}t}$ est négative. Ainsi $S(t)$ est décroissante et $S_{max} = S_0$,*
- *γ, $I(t)$ et N sont positifs, donc $\frac{\mathrm{d}R(t)}{\mathrm{d}t}$ est positive. Ainsi $R(t)$ est croissante et $R_{max} = R_{(\infty)}$.*

Ainsi, il est logique d'affirmer que le nombre de personnes susceptibles diminuera au cours du temps, alors que le nombre de personnes guéries augmentera au cours de l'épidémie. La vitesse de variation dépend alors du taux de transmission β et de la durée d'infection $\frac{1}{\gamma}$, autrement dit, du R_0.

Pour ce qui est de la fonction I, l'analyse est plus délicate car elle n'est pas strictement monotone.

Proposition 3. ***Variation de la fonction*** $I(t)$

$$\frac{\mathrm{d}i(t)}{\mathrm{d}t} = \frac{\beta s(t) i(t) - \gamma i(t)}{N} = \frac{\gamma i(t)}{N}\left(\frac{\beta i(t) s(t)}{\gamma i(t)} - 1\right) = \frac{\gamma i(t)}{N}(R_e(t) - 1)$$

Or $\gamma i(t)$ est positif. Ainsi, on peut déterminer la variation de $i(t)$ selon la valeur de R_t

- *si $R_e(t) > 1$, $i'(t)$ est positive donc $i(t)$ est alors croissante,*
- *si $R_e(t) < 1$, $i'(t)$ est négative donc $i(t)$ est alors décroissante,*
- *si $R_e(t) = 1$, $i'(t)$ est nulle donc $i(t)$ est constante. Par définition, $i(0) = 0$ et $i(\infty) = 0$. Ainsi, d'après le théorème des valeurs extrêmes, $i(t)$ atteint son maximum qu'on appellera i_{max}.*

Les variations de I permettent donc de mieux appréhender une épidémie. En effet, la première conséquence d'une maladie infectieuse est l'augmentation soudaine du nombre d'individus infectés. La connaissance de i_{max} permet donc de connaître le nombre maximum d'individus infectés au même moment et d'éviter que le milieu hospitalier soit submergé par le nombre de malades. Enfin, les basculements des variations de $I(t)$ engendrent une meilleure compréhension de l'indicateur du taux basique (et effectif) de reproduction.

Théorème 3.

- si $R_0 > 1$, une personne infectée contaminera plus d'une nouvelle personne. Dans ce cas, la maladie va se propager dans la population et pourra devenir épidémique,
- si $R_0 = 1$, une personne infectée contaminera une personne. Dans ce cas, le nombre de nouveaux cas est proportionnel au nombre d'individus guéris (ou décédés),
- si $R_0 < 1$, une personne infectée contaminera une personne au plus. Dans ce cas, le nombre de nouveaux cas déclinera rapidement et la maladie disparaîtra.

Il en est de même pour $R_e(t)$. Il suffit de connaître la proportion de personnes encore exposé à la maladie pour connaître ce taux de reproduction. Plus le nombre de personnes présentes dans le compartiment S diminue, plus le $R_e(t)$ diminue, puisqu'une personne infectée ne peut pas contaminer une personne déjà infectée ou guérie.

Enfin, le modèle SIR permet de connaître le nombre maximum d'individus infectés par rapport au taux basique de reproduction R_0. Comme affirmé précédemment, cette information peut être capitale dans la gouvernance d'une épidémie. La surcharge du milieu hospitalier est une analogie à la capacité de l'assureur à prendre en charge tous les sinistres de ses assurés arrivant au même instant. Cela permet donc à l'assureur de mieux se positionner sur les coûts marginaux que peut engendrer un nouvel assuré dans son portefeuille.

Proposition 4. ***Valeur de*** i_{max}

Même si le système d'équations différentielles du modèle SIR ne peut être résolu explicitement, il est possible d'obtenir une formule de i_{max} dépendant seulement de R_0.
En divisant la dérivée de i par rapport à la dérivée de s, on obtient :

$$\frac{\mathrm{d}i/\mathrm{d}t}{\mathrm{d}s/\mathrm{d}t} = \frac{\mathrm{d}i}{\mathrm{d}s} = -1 + \frac{\gamma}{\beta s}$$

Le résultat précédent est intégrable pour $i > 0$ tel que :

$$\int_0^t \mathrm{d}i = \int_0^t -1 + \frac{\gamma}{\beta s}\mathrm{d}s$$

En intégrant, on obtient donc la formule suivante pour tout $t \geqslant 0$:

$$i(t) - i(0) = -s(t) + \frac{\gamma}{\beta}\log s(t) + s(0) - \frac{\gamma}{\beta}\log s(0)$$

$$\Leftrightarrow i(t) + s(t) - \frac{\gamma}{\beta}\log s(t) = i(0) + s(0) - \frac{\gamma}{\beta}\log s(0)$$

$$\Leftrightarrow i(t) = i(0) + s(0) - s(t) + \frac{\gamma}{\beta}\log\frac{s(t)}{s(0)}$$

Puisque à $t = 0$, aucun individu est guéri (ou décédé) (i.e. $r(0) = 0$), on a $i(0) + s(0) = 1$. Ainsi :

$$i(t) = 1 - s(t) + \frac{\gamma}{\beta}\log\frac{s(t)}{s(0)}$$

Or $i(\infty) = 0$ (i.e.. quand l'épidémie est terminée, il n'y a plus d'individus infectés), on a l'équation transcendante :

$$1 - s(\infty) + \frac{\gamma}{\beta}\log\frac{s(\infty)}{s(0)} = 0$$

En rappelant que $R_0 = \frac{\beta}{\gamma}$, la formule précédente permet d'obtenir l'équation suivante :

$$R_0 = \frac{1}{s(\infty) - 1}\log(\frac{s(\infty)}{s(0)})$$

Ce résultat permet de mieux observer la valeur du R_0 selon la proportion de personnes saines à la fin de l'épidémie. Plus la proportion d'individus dans s est faible à la fin de l'épidémie, plus le R_0 est élevé. La figure suivante permet d'observer l'évolution du R_0 selon le $s_(\infty)$ en supposant que $s(0) = 99,99\%$.

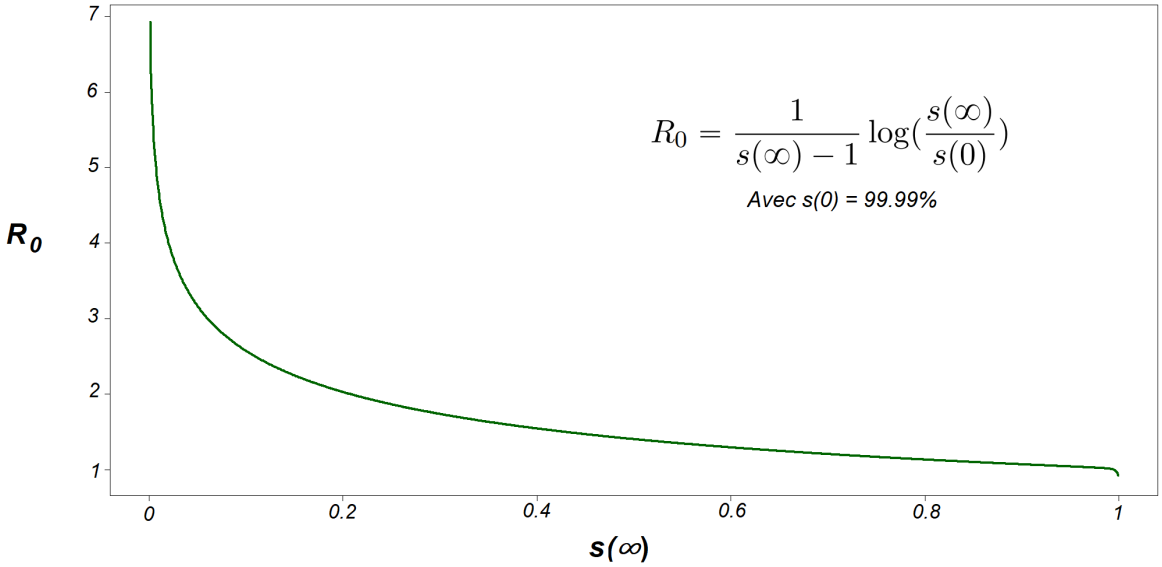

FIGURE 2.9 – Valeur du R_0 selon la proportion de personnes saines à la fin de l'épidémie avec $s(0) = 99,99\%$.

En revenant à l'équation de $i(t)$, il est possible de la "généraliser" pour s telle que :

$$i(s) = 1 - s + \frac{\gamma}{\beta}\log\frac{s}{s(0)}$$

Enfin quand $\frac{\mathrm{d}i}{\mathrm{d}t} = 0$, la valeur de $i(t)$ est i_{max} d'après la proposition 3 et ce maximum est atteint lorsque $R_e(t) = 1$. Autrement dit, c'est le moment où $s = \frac{1}{R_e(t)}$. En supposant que $s(0)$ tend vers 1 quand la population est grande, on a $s = \frac{\gamma}{\beta s(0)} = \frac{\gamma}{\beta}$.

Ainsi, on obtient la valeur de i_{imax}, telle que :

$$i_{max} = i(0) + s(0) - \frac{\gamma}{\beta}\log s(0) - \frac{\gamma}{\beta} + \frac{\gamma}{\beta}\log(\frac{\gamma}{\beta})$$

$$i_{max} = 1 - \frac{1}{R_0}(1 + \log R_0)$$

2.2.4.4 La taille finale de l'épidémie

Les épidémies finissent par disparaître car le nombre de personnes saines tend à décroître suffisamment pour que la maladie ne soit plus assez "contagieuse" (au sens du $R_e(t)$). Logiquement quand $S(\infty) = 0$, autrement dit, quand il n'y a plus aucune personne saine, l'épidémie est terminée. Toutefois, il est possible de démontrer que ce phénomène est impossible.

Proposition 5. *En divisant la dérivée de s par rapport à la dérivée de r, on obtient :*

$$\frac{\mathrm{d}s/\mathrm{d}t}{\mathrm{d}r/\mathrm{d}t} = \frac{\mathrm{d}s}{\mathrm{d}r} = \frac{-\beta si}{\gamma i} = \frac{-\beta s}{\gamma}$$

Le résultat précédent est intégrable pour $s > 0$ tel que :

$$\int_0^t \frac{1}{s}\mathrm{d}s = -\int_0^t \frac{\beta}{\gamma}\mathrm{d}r$$

En intégrant, on obtient donc la formule suivante pour tout $t \geqslant 0$:

$$s(t) = s(0)\exp\left(-\frac{\beta}{\gamma}(r(t) - r(0))\right)$$

Puisque au début de l'épidémie, aucun individu n'est guéri (ou décédé) (i.e. $r(0) = 0$), et $r(t) \leqslant 1$ (car $s(t) + i(t) + r(t) = 1$, on a $\forall t$: $s(t) \geqslant s(0)\exp(-\frac{\beta}{\gamma}) > 0$ Et donc, par définition on obtient l'équation suivante :

$$s(\infty) \geqslant s(0)\exp\left(-\frac{\beta}{\gamma}\right) > 0$$

Au fur et à mesure qu'une épidémie progresse, le nombre d'individus sains diminue et, par conséquent, le taux d'apparition de nouvelles infections diminue également. L'épidémie s'arrêtera donc avant que toute la population ne soit infectée.

L'objectif final de la taille de l'épidémie est donc de connaître le nombre cumulé de personnes infectées au cours de l'épidémie. Pour cela, il est possible de réduire l'équation transcendante $s(t) = s(0)\exp(-\frac{\beta}{\gamma}(r(t) - r(0)))$ tel que :

$$s(\infty) = s(0)\exp\left(-\frac{\beta}{\gamma}(r(\infty))\right) = s(0)\exp\left(-\frac{\beta}{\gamma}(1 - s(\infty))\right)$$

avec $i(\infty) = 0$

En passant au log, on a :

$$\log s(\infty) = R_0(s(\infty) - 1)$$

On retrouve la formule de la figure précédente, à la différence que $s(0)$ est arrondi à 1. Cette nouvelle équation peut être résolue de manière numérique afin d'obtenir le graphique suivant :

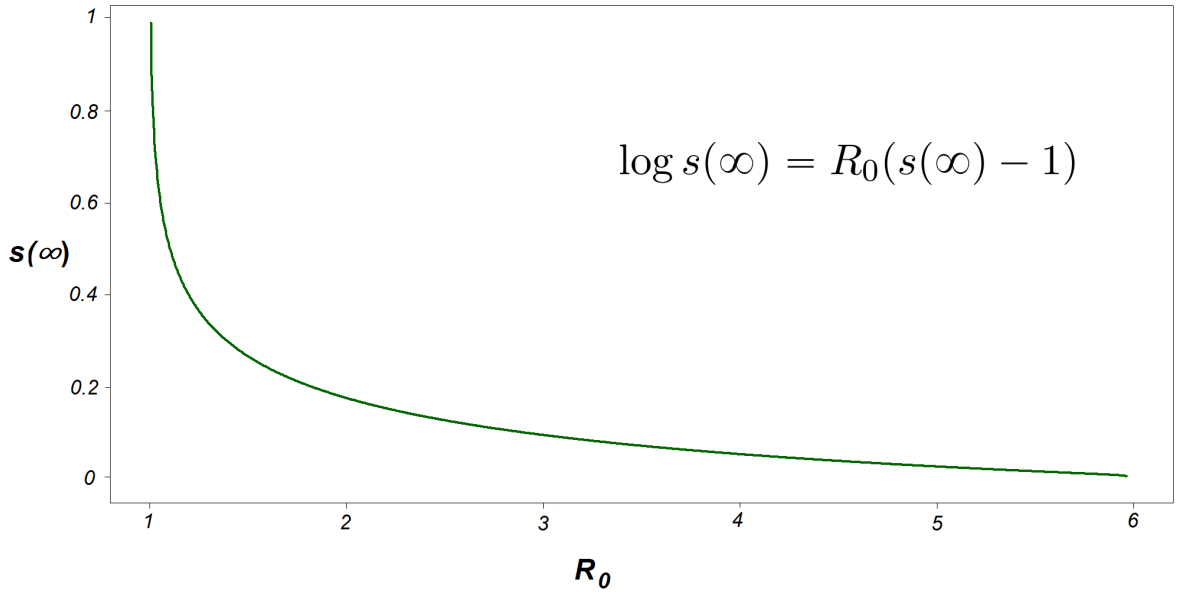

FIGURE 2.10 – Le nombre de personnes saines restantes selon le R0

Finalement, il est concluant d'affirmer que la taille finale de l'épidémie correspond à $1 - s(\infty)$ et il est possible de déterminer $s(\infty)$. Pour rappel, il a été démontré que $\forall t \geqslant 0$:

$$s(t) - \frac{\gamma}{\beta} \log s(t) - s(0) + \frac{\gamma}{\beta} \log s(0) = i(0) - i(t)$$

Cela est donc équivalent à dire que :

$$s(\infty) - \frac{\gamma}{\beta} \log s(\infty) - s(0) + \frac{\gamma}{\beta} \log s(0) = i(0) - i(\infty)$$

De plus $i(\infty) = 0$ puisqu'une épidémie tend toujours à disparaître. Ainsi on a :

$$\log \frac{s(\infty)}{s(0)} = \frac{\beta}{\gamma}(s(\infty) - s(0) - i(0))$$

$$\Leftrightarrow s(\infty) = s(0) \exp \frac{\beta}{\gamma}(s(\infty) - s(0) - i(0))$$

Il est désormais possible de définir une fonction telle que :

$$g(x) = s(0) \exp \frac{\beta}{\gamma}(x - s(0) - i(0))$$

où $g(x)$ est positive, croissante, strictement convexe et $g(s(0)) < s(0)$. Ainsi $s(\infty)$ est l'unique point de g inclut dans $[0, s(0)]$. Numériquement, il est donc possible de déterminer $s(\infty)$ avec :

$$s(\infty) = \lim_{n \to +\infty} g^n(s(0))$$

où $g^n(x)$ est la puissance fonctionnelle d'elle-même. Cette fonction est très utile puisqu'elle permet de connaître la taille finale du modèle SIR simple.

Dans le modèle SIR déterministe (où les paramètres sont fixés), on peut affirmer que le nombre maximum d'infectés est connu et qu'il n'y a qu'un seul pic d'infection. Cependant, dans la réalité, la taille finale d'une épidémie, i.e, le nombre d'individus sains qui finissent par contracter la maladie, ne se caractérise pas par un seul pic d'infectés. De nombreuses études ont justement montré l'inverse. À titre d'exemple, la pandémie de la Covid-19 se singularise par des vagues d'infection. Les oscillations de $I(t)$ peuvent s'expliquer par l'importation multiple d'individus infectés, des changements dans les interventions de santé publique (Sarakorn-Tang [19]), ou la prise en compte des variations géographiques (Rass-Radcliffe [18]). Les modèles compartimentaux multi-groupes permettent de s'adapter à cette contrainte des pics multiples pour $I(t)$ (Pierre Magal, Ousmane Seydib, Glenn Webb [12]).

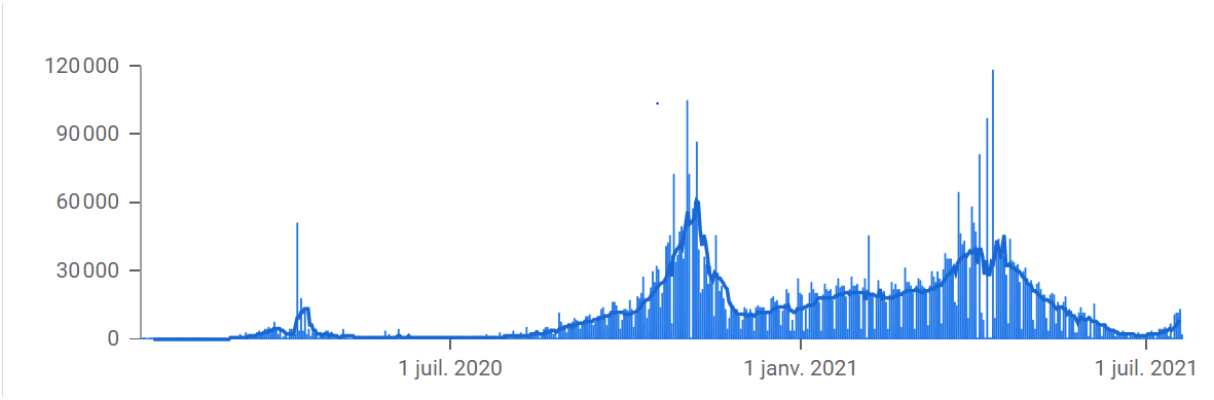

FIGURE 2.11 – La courbe $I(t)$ des infectés de la Covid-19 en France selon le temps et ses différents pics.

2.2.4.5 Notion supplémentaire du modèle SIR

L'âge demeure un facteur capital à prendre en compte lors de la modélisation de la propagation de certaines maladies. À titre d'exemple, la propagation du VIH est très fortement corrélée à l'âge. En effet, la transmission restante majoritairement sexuelle, les enfants sont rapidement exclus de la cause de propagation. De plus, il est logique d'admettre que les rapports sexuels ont tendance à regrouper deux individus d'un âge similaire. C'est ainsi qu'il existe des modèles SIR qui sont structurés par âge. Cette structuration n'a bien sûr aucune analogie avec la diffusion des rançongiciel. Néanmoins, une structuration par un autre facteur, comme la zone géographique peut être pertinente.

Définition 4. On appelle $s(t,a)$ (resp $i(t,a)$ et $r(t,a)$ un compartiment dépendant du temps t, mais également de l'âge a.

Définition 5. On définit $\lambda(t,a)$ la force de l'infection dépendant du temps t et de l'âge a, où la population est considérée comme continue par rapport à l'âge, tel que :

$$\lambda(t,a) = \int_0^{a_{max}} \beta(a,x) i(t,x) dx$$

où $\beta(a,x)$ est le taux avec lequel des individus sains d'âge a sont en contact avec des individus infectés d'âge x. On supposera que le taux de guérison γ est constant quel que soit l'âge.

La population étant considérée comme continue par rapport à l'âge, λ est calculé à partir d'une intégrale. Finalement, on somme le nombre de personnes *susceptibles* qui vont devenir infectées au contact d'individus de tout âge. Ceci dit, il est tout à fait envisageable d'utiliser une somme pour une variable catégorielle, comme par exemple la zone géographique.

Proposition 6. *Le paramètre $\beta(a,x)$ est probabilisé. Généralement, une gausienne centrée en a et de variance σ^2 est choisie pour $\beta(a,x)$, tel que :*

$$\beta(a,x) = \frac{1}{\sigma\sqrt{2\pi}} \exp^{-\frac{(a-x)^2}{2\sigma^2}}$$

Ainsi, dans ce modèle, il est considéré qu'il est plus probable qu'une personne contamine un individu d'un âge proche.

Proposition 7. *La dynamique de l'épidémie s'écrit donc en fonction du temps t et de l'âge a, telle qu'elle soit décrite par le système d'équations différentielles suivant :*

$$\begin{cases} \frac{\partial S(a,t)}{\partial t} + \frac{\partial S(a,t)}{\partial a} = -\lambda(a,t)S(a,t) \\ \frac{\partial I(a,t)}{\partial t} + \frac{\partial I(a,t)}{\partial a} = \lambda(a,t)S(a,t) - \gamma I(a,t) \\ \frac{\partial R(a,t)}{\partial t} + \frac{\partial R(a,t)}{\partial a} = \gamma I(a,t) \end{cases}$$

2.3 Le modèle SIR multi-groupes

2.3.1 Description et utilité

Le modèle SIR multi-groupes a pour objectif d'intégrer une variable qualitative permettant de diviser la population selon ce critère. Dans le cadre d'une épidémie dûe à un agent pathogène, un facteur discriminant, comme la zone géographique, est un moyen de séparer la population totale. Il existe donc toujours une population exposée au virus, mais cette dernière est divisée en plusieurs groupes ayant tous un facteur en commun. L'idée principale est donc de supposer que certains groupes d'individus ont peut-être plus de probabilité de communiquer que d'autres groupes. Ainsi, les paramètres β et γ régissant la propagation de l'épidémie ne sont plus universels. À contrario pour chaque relation entre deux groupes (ainsi que pour lui-même), un β et un γ propre à cette liaison est nécessaire. Plus précisément, il existe pour k groupes, k^2 β et k^2 γ. Pour illustrer les propos, la figure suivante propose un schéma de modèle SIR à deux groupes :

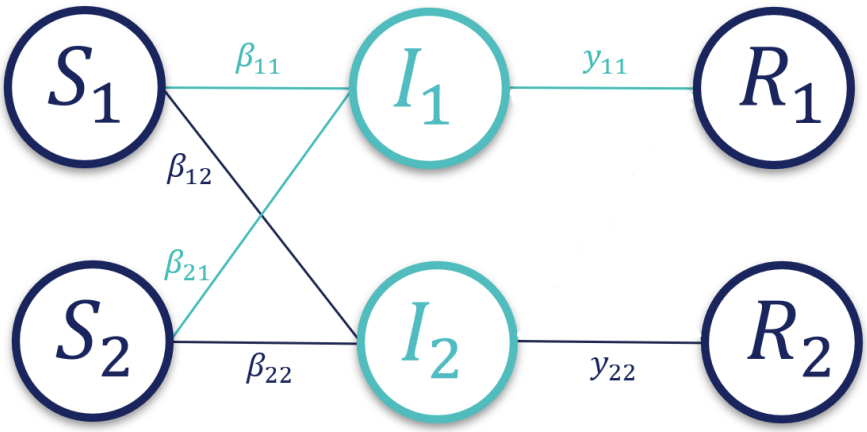

FIGURE 2.12 – Schéma des compartiments d'un modèle SIR à 2 groupes

Le fonctionnent du modèle est le suivant : Les populations sont divisées en deux catégories selon un facteur. Ainsi une partie de la population appartient à S_1, alors que l'autre appartient à S_2. L'épidémie

démarre quand un infecté apparaît. Supposons qu'il soit du premier groupe. Il y a donc un individu dans I_1. Cet individu peut contaminer la population S_1 et S_2, mais le taux de transmission est propre à chaque groupe selon le facteur les séparant. Une fois qu'un individu du groupe 2 est infecté, alors le fonctionnement est symétrique au précédent. Enfin dès que la durée de guérison prend fin, l'individu infecté rejoint le compartiment R de son groupe.

Ce type de modélisation engendre plusieurs avantages. Le premier réside dans la précision de la propagation. Si les données et les informations de la variable séparatrice sont précises, alors la représentation globale de la diffusion de l'épidémie le sera également. Rappelons que β correspond au taux de transmission et γ au taux de guérison. Si la variable séparatrice est par exemple l'âge, il est légitime de stipuler que le nombre de contacts d'un individu de 20 ans n'est pas le même que celui d'une personne de 80 ans. Ainsi, leur taux de transmission n'est pas du tout identique et le modèle multi-groupes permet de palier la généralisation des paramètres qui semble finalement peu représentative de la réalité. De plus, comme décrit dans la section précédente, la forme d'une épidémie ne contient pas un seul pic d'infectés, mais plutôt à plusieurs vagues d'épidémie. Ainsi, le deuxième avantage du modèle est sa capacité à reproduire les vagues épidémiques.

2.3.2 Analyse du modèle SIR multi-groupes

L'objectif de cette section est de proposer une continuité à l'analyse du modèle SIR simple et d'obtenir si possible la taille finale de l'épidémie. Pour cela, il sera supposé que le modèle SIR est composé de n groupes différents.

2.3.2.1 Notations :

- Soit N un vecteur de taille n groupes composé de chaque groupe de population exposée à l'épidémie. N représente donc la population totale du modèle tel que

$$N = \begin{pmatrix} N_1 \\ \vdots \\ N_n \end{pmatrix}$$

où $(N_1 \dots N_n)$ est égale à la population totale de chaque sous-groupes.

- Soit S, I et R des vecteurs de taille n représentant les 3 compartiment de chaque groupe. Ainsi, il est possible d'écrire ces vecteurs tels que :

$$S = \begin{pmatrix} S_1 \\ \vdots \\ S_n \end{pmatrix}, I = \begin{pmatrix} I_1 \\ \vdots \\ I_n \end{pmatrix} \text{ et } R = \begin{pmatrix} R_1 \\ \vdots \\ R_n \end{pmatrix}$$

où $(S_1 \dots S_n)$ $(I_1 \dots I_n)$ $(R_1 \dots R_n)$ sont des fonctions telles que définies dans la proposition 1. De plus, il est noté que $N(t) = S(t) + I(t) + R(t) \forall t \geqslant 0$, tel que :

$$\begin{pmatrix} N_1(t) \\ \vdots \\ N_n(t) \end{pmatrix} = \begin{pmatrix} S_1(t) \\ \vdots \\ S_n(t) \end{pmatrix} + \begin{pmatrix} I_1(t) \\ \vdots \\ I_n(t) \end{pmatrix} + \begin{pmatrix} R_1(t) \\ \vdots \\ R_n(t) \end{pmatrix}$$

- De la même façon que dans le modèle SIR simple, on note que s, i et r sont les fractions de

personnes de chaque compartiment tel que :

$$s = \begin{pmatrix} \frac{S_1}{N_1} \\ \vdots \\ \frac{S_n}{N_n} \end{pmatrix}, i = \begin{pmatrix} \frac{I_1}{N_1} \\ \vdots \\ \frac{I_n}{N_n} \end{pmatrix} \text{ et } r = \begin{pmatrix} \frac{R_1}{N_1} \\ \vdots \\ \frac{R_n}{N_n} \end{pmatrix}$$

- B correspond à la matrice des taux de transmission, tel que :

$$B = \begin{pmatrix} \beta_{1,1} & \dots & \beta_{1,n} \\ \vdots & \ddots & \vdots \\ \beta_{n,1} & \dots & \beta_{n,n} \end{pmatrix}$$

où $\beta_{i,j}$ (avec $(i,j) \in [0,n]^2$) correspond au taux de transmission des individus du groupe i contaminant les individus du groupe j.

Cette matrice est à coefficients positifs. Si tous les coefficients non diagonaux sont strictement positifs alors la matrice B est irréductible.

- E est la matrice des taux de guérison, tel que :

$$E = \begin{pmatrix} \gamma_{1,1} & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & \gamma_{n,n} \end{pmatrix}$$

où $\gamma_{i,i}$ correspond au taux de guérison des personnes appartenant au groupe i. Ce taux permet le passage entre le compartiment I_i et R_i. La matrice E est supposé diagonale, car il est impossible de passer d'un compartiment I dans un groupe précis à un compartiment R d'un autre groupe. En d'autres termes, le fait de guérir de la maladie est totalement indépendant de la propagation de la maladie dans les autres groupes.

2.3.2.2 Dynamique du modèle SIR multi-groupes :

De la même manière que pour le modèle SIR simple, la dynamique de ce modèle est décrite par le système d'équations différentielles suivant régissant la propagation de l'épidémie $\forall t \geqslant 0$:

$$\begin{cases} \dfrac{\mathrm{d}S(t)}{\mathrm{d}t} = -S(t)BI(t) \\ \dfrac{\mathrm{d}I(t)}{\mathrm{d}t} = S(t)BI(t) - EI(t) \\ \dfrac{\mathrm{d}R(t)}{\mathrm{d}t} = EI(t) \end{cases}$$

avec comme conditions initiales que $S(0) \in \mathbf{R}_+^n$, $I(0) \in \mathbf{R}_+^n$ et $R(0) \in \mathbf{R}_+^n$ et $N(0) = S(0) + I(0) + R(0)$

Cette écriture matricielle des équations différentielles des vecteurs n'est pas l'unique moyen de décrire la dynamique de l'épidémie. Il est tout à fait possible de s'intéresser aux équations différentielles d'un seul groupe. Ainsi, pour le groupe k, avec $k = 1, ..., n$, la dynamique $\forall t \geqslant 0$ est la suivante :

$$\begin{cases} \dfrac{\mathrm{d}S_k(t)}{\mathrm{d}t} = -S_k(t)\sum_{j=1}^{n}\beta_{k,j}\ I_j(t) \\ \dfrac{\mathrm{d}I_k(t)}{\mathrm{d}t} = S_k(t)\sum_{j=1}^{n}\beta_{k,j}\ I_j(t) - \gamma_k I_k(t) \\ \dfrac{\mathrm{d}R_k(t)}{\mathrm{d}t} = \gamma_k I_k(t) \end{cases}$$

2.3.2.3 La taille finale d'une épidémie d'un modèle multi-groupes

Comme démontrer dans l'analyse du modèle SIR simple, cette section a pour but d'obtenir la taille finale de l'épidémie. En utilisant les équations différentielles précédentes, on obtient pour $k = 1, ..., n$:

$$\frac{\mathrm{d}\log S_k(t)}{\mathrm{d}t} = \frac{1}{S_k(t)}\frac{\mathrm{d}S_k(t)}{\mathrm{d}t} = -\sum_{j=1}^{n}\beta_{k,j}\ I_k(t)$$

$$\implies \log\frac{S_k(t)}{S_k(0)} = \sum_{j=1}^{n}\beta_{k,j}\int_0^t I_k(s)\mathrm{d}s \tag{2.1}$$

De la même façon, la somme des équations de S_k et de I_k permet d'obtenir la formule suivante $\forall t > 0$:

$$(S_k + I_k)(t) - (S_k + I_k)(0) = -\gamma_k\int_0^t I_k(s)\mathrm{d}s \tag{2.2}$$

En combinant l'équation (2.1) et (2.2), on obtient une relation entre le nombre de susceptibles et de personnes infectées à l'instant t et au départ de l'épidémie :

$$\sum_{j=1}^{n}\frac{\beta_{kj}}{\gamma_j}(S_j(0) + I_j(0)) - \log(S_k(0)) = \sum_{j=1}^{n}\frac{\beta_{kj}}{\gamma_j}(S_j(t) + I_j(t)) - \log(S_k(t))$$

Et cette dernière équation permet de revenir à la forme d'une dérivée partielle telle que :

$$\frac{\mathrm{d}}{\mathrm{d}t}[\sum_{j=1}^{n}\frac{\beta_{kj}}{\gamma_j}(S_j(t) + I_j(t)) - \log(S_k(t))] = 0$$

Il est désormais possible d'intégrer la dernière équation entre 0 et $+\infty$ pour $k = 1, .., n$ et de retrouver des équations transcendantes comme dans le cadre du modèle SIR simple. On obtient alors :

$$F_k(X) = S_k(0) * \exp(\sum_{j=1}^{n}\frac{\beta_{kj}}{\gamma_j}(X_j - S_j(0)) - \sum_{j=1}^{n}\frac{\beta_{kj}}{\gamma_j}I_j(0))$$

Cette relation permet donc de connaître la taille finale de l'épidémie. Cependant, comme démontrer dans [12], l'utilisation de cette fonction nécessite que la matrice B soit irréductible et strictement positive.

Pour conclure, l'avantage du modèle SIR multi-groupes comparé au modèle simple réside dans trois points :

— une meilleure précision dans la propagation du virus,
— plusieurs pics d'infections représentant mieux la réalité des vagues épidémiques,
— la modélisation possible d'individus considérés comme "supraconducteurs", c'est à dire, d'individus qui vont infecter un nombre important d'individus sains.

2.4 Théorie des graphes et spectre laplacien

La théorie des graphes est une branche des mathématiques et de l'informatique qui a pour objectif d'étudier la structure d'un réseau représenté sous forme de graphe. Ces modèles de dessins de réseaux peuvent décrire de nombreux concepts tels qu'un réseau d'ordinateurs, des routes entre des villes, des réseaux sociaux, ou encore des structures génétiques. Les applications des graphes sont en réalité plus larges qu'il n'y paraît. En effet, de nombreuses problématiques mathématiques ont eu recours à cette théorie afin d'obtenir une réponse. Par exemple, le théorème des quatre couleurs, qui indique que seulement quatre couleurs différentes sont nécessaires pour colorier n'importe quelle carte découpée en zones connexes, utilise la théorie des graphes dans le cadre de son algorithme de résolution. Avant d'exprimer l'intérêt de cette théorie dans l'avancée de ce mémoire, il semble judicieux de définir quelques notions propres à ce sujet.

2.4.1 Éléments et concepts de la théorie des graphes

Afin de saisir tous les principes de cette branche mathématiques, il est nécessaire de définir mathématiquement un graphe :

Noté G, un graphe est caractérisé par un ensemble de sommets V et un ensemble d'arêtes, également appelé liens, E. Ainsi, G correspond aux ensembles (V, E), tel que $G = (V, E)$. Il est également possible d'ajouter un poids sur chaque arête. Généralement, plus le poids est important, plus la connexion entre deux sommets est forte. Cependant, il est également possible de voir ce poids comme la distance euclidienne séparant deux sommets. Ainsi, on notera alors W un vecteur de poids tel que le graphe est donné par $G = (V, E, W)$.

— le nombre de sommets d'un graphe est noté $n = |V|$,
— le nombre d'arêtes d'un graphe est noté $m = |E|$,
— di 2 sommets a et b sont adjacents, alors l'arête est désigné par $(a; b)$ et $(a, b) \in E$,
— le degré d'un sommet correspond au nombre de sommets auquel il est relié. Le degré du sommet a est alors noté $d(a)$,
— un graphe est dit k-régulier lorsque $d(i) = k, \forall i\ inV$ avec k un entier naturel.

À partir de ces propriétés, il est possible de déterminer deux matrices donnant des informations sur le graphe : Étant donné un graphe $G = (V, E)$ où $n := |V|$ et v_i désignant les sommets de ce graphe avec $i = 1, .., n$, on définit la matrice de degrés D et la matrice d'adjacence A, de taille $n \times n$ telles que :

$$D = \begin{pmatrix} d(v_1) & \dots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \dots & d(v_n) \end{pmatrix}, A = \begin{pmatrix} 0 & \dots & \mathbf{1}_{(v_1,v_n)\in E} \\ \vdots & \ddots & \vdots \\ \mathbf{1}_{(v_n,v_1)\in E} & \dots & 0 \end{pmatrix}$$

Pour un graphe $G = (V, E, W)$, la matrice d'adjacence ne correspond pas à des indicatrices, mais à la valeur du poids entre deux sommets. Si les deux sommets ne sont pas reliés, alors la valeur vaut toujours 0.

Même si les potentiels domaines d'applications sont variés, l'idée principale est de représenter les relations entre plusieurs entités. Dans le cadre de la propagation des rançongiciels, l'objectif d'un graphe est de définir la relation des entreprises du portefeuille. Ainsi, la communication, la zone géographique et le secteur d'activités peuvent représenter la proximité entre deux assurés. Mathématiquement, l'entreprise correspond à un sommet et ses relations aux arêtes. À noter qu'il est équivalent de représenter les relations par des sommets et les arêtes par les entreprises. L'objectif est de pouvoir mesurer la connexion globale du graphe, afin de savoir à quel point ce dernier est connecté ou non. Il est également envisageable de regarder la connexion d'un sous graphe. Il faudra alors parler de connexion locale. C'est ici qu'interviennent les spectres laplaciens.

La matrice laplacienne L d'un graphe $G = (V, E)$ où $n = |V|$ est une matrice de taille $n \times n$ telle que

$$L = D - A$$

En d'autres termes, la diagonale de L exprime le degré des sommets de G et les coefficiants en dehors de la diagonale quantifie l'adjacence des sommets. D'ailleurs, la forme quadratique de cette matrice $x^t Lx = \sum_{(a,b)\in E} W_{a,b}(x(a) - x(b))^2$ indique que L est semi-définie positive.

Tout l'intérêt de cette matrice est que son spectre fournit des informations topologiques sur le graphe. Il permet d'évaluer et de quantifier la "connexion" d'un graphe. Puisque L est semi-définie positive et qu'elle est à valeur dans $\mathbb{R}$, le théorème spectrale justifie que L est diagonalisable et que ses valeurs propres sont réelles. En ordonnant de façon croissante les valeurs propres de L notées, λ_i $\forall i \in V$, λ_2 est appelé connectivité algébrique. En d'autres termes, la valeur de λ_2 qualifie la structure du graphe. Plus la valeur de λ_2 est forte, plus le graphe est alors connecté. Si $\lambda_2 = 0$ alors le graphe est dit non-connexe, c'est à dire qu'il n'est pas possible de circuler entre tous les sommets via les arêtes.

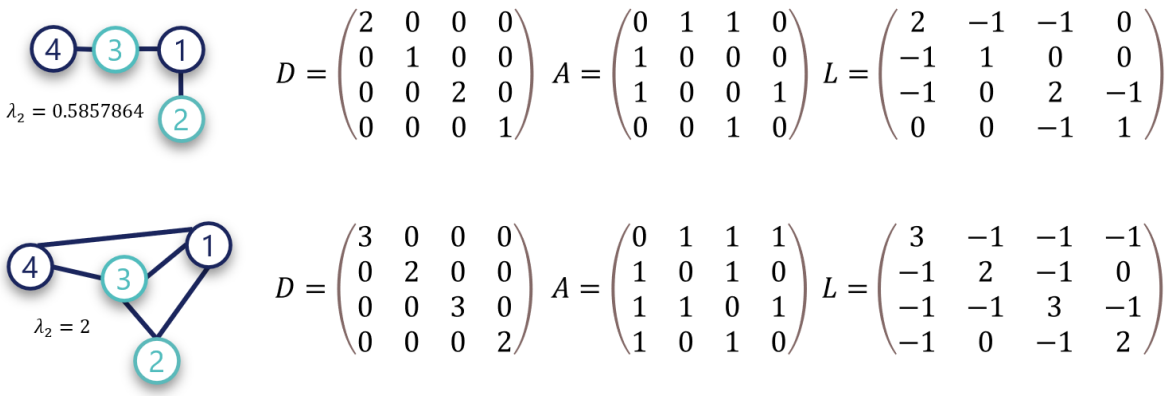

FIGURE 2.13 – Exemple de la matrice laplacienne et de la connectivité algébrique de deux graphes

Comme expliqué ci-dessus, la connectivité algébrique permet donc d'avoir une information sur la connexion globale du graphe. Cependant, il est également naturel de vouloir mesurer le degré de connexion d'un sous-graphe, c'est à dire à un sous-ensemble du graphe. Pour cela, il est nécessaire de définir deux notions.

Soit S, un sous-ensemble des sommets d'un graphe $G = (V, E)$ où a et b sont deux sommets du graphe ; la frontière $\partial(S)$ de S est l'ensemble des arêtes dont une extremité est dans S, alors que l'autre est hors de S. Mathématiquement, cette frontière est définie telle que :

$$\partial(S) = \{(a, b) \in E | a \in S, b \notin S\}$$

Ainsi, pour mesurer le degré de connexion de S au reste du graphe, il est possible de diviser la frontière $\partial(S)$ par le minimum des sommets dans S ou hors de S. Cette notion est notée $\theta(S)$ telle que :

$$\theta(S) = \frac{\partial(S)}{min(|S|, |V \backslash S)}$$

Le rapport isopérimétrique θ_G est alors donné par la valeur minimale de θ_G sur tous les sous-ensembles S contenant au plus la moitié des sommets, c'est-à-dire :

$$\theta_G = min\{\theta(S), |S| < \frac{n}{2}\}$$

Enfin, on obtient l'inéquation suivante, permettant d'avoir une information sur la connectivité algébrique :

$$\lambda_2 \leqslant 2\theta_G$$

Chapitre 3

Modélisation actuarielle

3.1 Introduction : le modèle collectif, une approche d'évènements d'accumulation

Le modèle classique de l'assurance non-vie en actuariat est souvent associé à la modélisation par le modèle individuel et le modèle collectif. Ce deuxième permet de modéliser des évènements aléatoires en fonction de la fréquence et de la sévérité.

Pour rappel, on note N, une variable aléatoire à valeur entière ($N \in \mathrm{N}$) associée à un générateur de fréquence permettant de simuler un nombre d'évènements aléatoires. Dans de nombreux cas, cette variable est distribuée selon une loi de Poisson de paramètre λ avec $\lambda > 0$, mais elle peut également l'être par d'autres distributions comme la loi binomiale, binomiale négative, ou la poisson distribuée. En d'autres termes, cette variable permet d'approcher la fréquence des sinistres de la modélisation.

Pour la sévérité, un second générateur est nécessaire ; celui des coûts associés à ces évènements. Il permet de simuler des évènements d'accumulation par une approche de coût. Il est noté X_i avec $i \in [\![1, N]\!]$. Cette variable est généralement associée à des lois continues positives, comme la loi Log-Normale ou de Pareto.

Enfin, il est possible de noter S, le coût total des évènements tel que :

$$S = \sum_{i=1}^{N} X_i$$

Le modèle classique suppose deux hypothèses :
- l'indépendance entre la fréquence et le coût des sinistres (N et X_i sont indépendants),
- indépendance et stationnarité des X_i (les coûts des sinistres sont indépendants et ne varient pas dans le temps).

Si les données disponibles sont assez complètes, le modèle peut être facilement calibré. Mais comme répété au fil du mémoire, le risque Cyber et particulièrement celui des rançongiciels souffrent d'un manque de données rendant l'utilisation de ce modèle délicat. De plus, ces hypothèses supposées ne correspondent pas à la réalité des rançongiciels s'auto-propageant, mais plutôt à ceux qui ciblent une victime en particulier. En effet, la propagation d'un *malware* au sein d'un portefeuille ne respecte pas ces hypothèses. Les évènements ne sont plus indépendants, mais corrélés. Même si, la première

infection de départ peut être externe au portefeuille, en supposant que le portefeuille est trop petit pour représenter la population des entreprises mondiales, la diffusion du rançongiciel repose plus sur un modèle déterministe où les évènements survenus sont une conséquence des évènements précédents. Ainsi, il semble plus judicieux de proposer un modèle actuariel propre à ce type de problématique.

3.2 Modélisation des coûts des sinistres en termes de DCP pour le risque Cyber

De nombreux travaux existants se sont tournés sur une modélisation du coût d'un évènement résultant d'une attaque Cyber. L'objectif de ce modèle repose essentiellement sur le coût engendré par des pertes de données, plus communément appelées DCP. Cette modélisation semble donc pertinente dans un scénario de type rançongiciel. En effet, une partie des coûts engendrés par ces sinistres sont dûs par la perte de données sensibles. Dans son mémoire *T.Bastard* [2] relate un premier modèle simple reposant sur des règles proportionnelles et des études *Ponemon et IBM* [15].

Soit α, β et γ, 3 constantes positives ou nulles, représentant des facteurs d'ajustement propres à l'entreprise tels que :

— secteur d'activités de l'entreprise α_{secteur},
— pays d'activité de l'entreprise β_{pays},
— taille de l'entreprise γ_{taille}.

Ces éléments permettent donc de constituer un premier modèle, tel que le coût total d'un évènement Cyber est directement lié au nombre de DCP perdues. Ainsi on a :

$$\text{Coût (secteur, pays, taille)} = \alpha_{\text{secteur}} \times \beta_{\text{pays}} \times \gamma_{\text{taille}} \times \text{Coût moyen}$$

Cependant, cette formule est basée sur une hypothèse de proportionnalité du coût et elle ne prend pas en compte la forte dispersion du risque. Elle sera rapidement remise en cause et de nouveaux modèles apparaîtront.

Ainsi, deux modèles de coût sont aujourd'hui proposés ne reposant plus sur la proportionnalité du coût du sinistre mais sur une structure prenant en compte le nombre de DCP et 3 paramètres à fixer (a, b et σ^2).

$$\log(\text{coût}) = a + b \times \log(\text{nb DCP}) + \epsilon \text{ (Jay Jacobs)}$$

$$\log(\text{coût}) = a + b \times \log(\log(\text{nb DCP})) + \epsilon \text{ (Farkas)}$$

où a et b sont des coefficients réels et $\epsilon \sim \mathcal{N}(0, \sigma^2)$.

Ces deux formules proposent des avantages et des inconvénients. Ces derniers sont détaillées par *T.Basard* [2]. Pour résumer, à nombre de DCP fixé, le coût est modélisé par une loi log-normale, mais seul le modèle *Jay Jacobs* est adapté aux petites et aux grandes pertes de DCP. Plus précisément, *Farkas* assumera que sa formule ne fonctionne pas autant qu'espéré et c'est donc pourquoi, il est plus pertinent de se concentrer sur la structure du modèle de *Jay Jacobs*.

En résumé, cette approche est nécessaire à la modélisation actuarielle de la propagation d'un rançongiciel. Elle permet de modéliser le coût de chaque sinistre en se basant seulement sur 1 variable qui est le nombre de données à caractère personnel perdues par l'attaque. Les coefficients a, b et ϵ sont à fixer.

Cette modélisation permet dans le cadre de la propagation d'un rançongiciel de détailler deux quantités :

— lors de la souscription, ces modélisations permettent à l'assureur d'obtenir rapidement le coût total des données qui peuvent être perdues en cas d'attaque massive de rançongiciel. Mise bout à bout, elles pourraient même donner un indice sur le coût total de DCP du portefeuille d'assurés,
— lors des simulations des scénarios d'attaque de rançongiciel, ces formules aident à constituer une estimation du coût de l'attaque Cyber.

3.3 Propagation d'un rançongiciel au sein d'un portefeuille

Comme expliqué dans les travaux de *C.Hillairet et al.* [8], l'objectif de cette section est de proposer une modélisation de l'impact d'une Cyber-attaque sur un portefeuille d'assurés. À l'aide de scénarios d'accumulation permettant d'évaluer la capacité à encaisser ce type d'attaque selon différents coûts et comportements,

3.3.1 Modélisation des effets d'une attaque par rançongiciel sur un portefeuille d'assuré

Supposons un portefeuille d'assuré constitué de N entreprises. Lors d'un évènement de rançongiciel s'auto-diffusant, ce portefeuille peut être affecté de plusieurs manières :

— un des assurés est infecté par une entreprise (dans ou en dehors du portefeuille),
— après infection, l'assuré ne nécessite plus l'aide de l'assureur,
— un des assurés est immunisé contre le rançongiciel avant qu'il ait été infecté grâce à une stratégie de protection.

Quand la crise de rançongiciel est déclarée (le temps 0 représente cet instant), chaque assuré a une probabilité d'être infecté à chaque instant. On note T_j, avec $j \in [\![1, N]\!]$, le temps auquel l'assuré j est infecté. Ainsi, quand un assuré est infecté, l'assureur se doit de lui porter assistance de plusieurs manières. La première aide sera de type financière, alors que les autres aides sont des actions permettant de réduire le temps pendant lequel l'assuré a définitivement stoppé son activité à cause de l'attaque. Comme expliqué lors du premier chapitre, de nombreuses garanties proposent l'intervention d'une entreprise de Cyber-sécurité en partenariat avec l'assureur. Ainsi, on notera U_j la durée d'assistance que l'assuré j nécessite. À partir de ces deux variables, il est possible de construire l'instant auquel l'assuré j ne nécessitera plus d'assistance de la part de l'assureur. Ce moment est noté $T_j + U_j$. Le vecteur aléatoire $(T_j, U_j)_{1 \leqslant j \leqslant n}$ est supposé indépendant et identiquement distribué. Néanmoins l'hypothèse d'indépendance peut être contesté, puisqu'on peut supposer qu'un assuré du portefeuille contamine directement un autre assuré. En supposant que le portefeuille soit d'une taille spécifique et que la politique de souscription évite des entreprises dites à *cluster*, alors la supposition que l'infection vienne de l'extérieur demeure correcte.

De la même manière qu'expliqué au cours de ce mémoire, un assuré peut être considéré immunisé contre l'attaque avant qu'il ne soit infecté. Cette analogie au vaccin passe par des fortes mesures de sécurité sur le parc informatique de l'assuré, ainsi que sur la formation de ses employés à la Cyber-sécurité. De plus, une fois infecté, l'assuré sera considéré comme immunisé contre ce rançongiciel. Ainsi, à un instant précis, l'assuré j peut être immunisé contre l'attaque. On note ce moment C_j. De la même façon que pour U et T, $(C_j)_{1 \leqslant j \leqslant n}$ est supposé indépendant et identiquement distribué. De plus, il sera

supposé que les trois variables T, U et C sont indépendantes et sont des variables de durées. Elles possèdent donc un taux de hasard tel qu'une variable aléatoire continue A possède un taux de hasard noté λ_A défini comme :

$$\lambda_A(t) = \lim_{\mathrm{d}t \to 0^+} \frac{1}{\mathrm{d}t} \mathbb{P}(A \in [t, t + \mathrm{t}] | A \geqslant t)$$

Pour savoir si l'assuré j a été immunisé avant d'être infecté, on notera deux éléments permettant de différencier cette singularité :

— $Y_j = \inf(C_j, T_j)$: Le temps auquel l'assuré ne peut plus être affecté par le rançongiciel,
— $\delta_j = \mathbb{1}_{T_j \leqslant C_j}$: Si l'assuré a été infecté avant d'être immunisé.

Le tableau suivant résume toutes les variables introduites dans cette sous-section :

Variable	**Signification**
Tj	Temps auquel l'assuré j est infecté
Uj	Durée de l'assistance pour l'assuré j
Tj + Uj	Temps auquel l'assuré j n'a plus besoin d'assistance
Cj	Temps auquel l'assuré j est immunisé
$Y_j = \inf(C_j, T_j)$	Temps auquel l'assuré j est soit immunisé, soit infecté
$\delta_j = \mathbb{1}_{T_j \leqslant C_j}$	Indique si l'assuré j a été infecté avant d'être immunisé
$\lambda_A(t)$	Taux de hasard de la variable aléatoire continue A

3.3.2 Modélisation de la propagation

Comme décrit dans la section précédente, la modélisation de la propagation repose sur le modèle SIR multi-groupes. L'objectif est donc de diviser notre portefeuille en plusieurs groupes selon le secteur d'activités de l'entreprise. Avec L, un entier strictement positif, représentant le nombre de secteur d'activités différent, il est possible de créer L groupe homogène par rapport à cette variable dans notre modèle SIR multi-groupes. Pour rappel, les équations différentielles décrivant la dynamique de la propagation sont les suivantes :

$$\begin{cases} \dfrac{\mathrm{d}S_k(t)}{\mathrm{d}t} = -S_k(t) \sum_{j=1}^{n} \beta_{k,j}\ I_j(t) \\ \dfrac{\mathrm{d}I_k(t)}{\mathrm{d}t} = S_k(t) \sum_{j=1}^{n} \beta_{k,j}\ I_j(t) - \gamma_k I_k(t) \\ \dfrac{\mathrm{d}R_k(t)}{\mathrm{d}t} = \gamma_k I_k(t) \end{cases}$$

Puisque T représente la force de contagion, il semble logique de supposer que son taux de hasard est décrit tel que :

$$\lambda_T(t) = \beta i_t$$

Néanmoins, le modèle SIR multi-groupes nécessite plusieurs paramètres β formant une matrice B. Ainsi, pour chaque groupe k et h avec $k, h \in \{2, .., L\}$ et $k \neq h$, il existe un taux de hasard $\lambda_T(t)_{k,h}$ tel que

$$\lambda_T(t)_{k,h} = \beta_{k,h} i_t^{k,h}$$

3.3.3 Impacts et coûts pour l'assureur

Afin de mesurer l'impact que le portefeuille peut avoir sur l'assureur, il semble pertinent de définir différentes mesures permettant d'avoir une observation sur l'évolution du portefeuille à n'importe quel instant de l'épidémie du rançongiciel.

La première mesure est donc celle du nombre cumulé d'assurés infectés à chaque instant t de l'épidémie. Elle permet de comprendre à quelle vitesse l'épidémie se propage et également le calcul d'un coût pour l'assureur. Ainsi, on note N_t le nombre cumulé d'assurés infectés à l'instant t, tel que :

$$\mathrm{N}_t = \sum_{j=1}^{n} \delta_j \mathbb{1}_{Y_j \leqslant t} = \sum_{j=1}^{n} \delta_j \mathbb{1}_{T_j \leqslant t}$$

Une autre mesure imaginable est celle du nombre d'assurés infectés qui sont guéris avant l'instant t. Cette mesure est notée :

$$\mathrm{R}_t = \sum_{j=1}^{n} \delta_j \mathbb{1}_{Y_j + U_j \leqslant t} = \sum_{j=1}^{n} \delta_j \mathbb{1}_{T_j + U_j \leqslant t}$$

La dernière mesure introduite dans cette partie est celle du nombre d'assurés infectés à l'instant t, qui en d'autres termes, n'est que la différence entre le nombre cumulé d'assurés infectés à t et nombre d'assurés infectés qui sont guéris avant l'instant t :

$$\mathrm{J}_t = \mathrm{N}_t - \mathrm{R}_t$$

Ces 3 mesures engendrent la possibilité de créer 3 coûts différents pour l'assureur.

Le premier coût noté C_1 représente le coût financier (Perte d'exploitation, DCP, coût matériel ect..) que l'assureur doit prendre en compte. C représente le coût moyen des sinistres. Ainsi, ce coût n'est que la multiplication du coût moyen par le nombre cumulé d'assurés infectés. Ce coût s'écrit alors :

$$\mathrm{C}_1 = C \sup_{t \geqslant 0} \mathrm{N}_t = C \lim_{t \to +\infty} \mathrm{N}_t$$

Le deuxième coût mesure la capacité maximum que l'assureur possède pour assister ces assurés. En d'autres termes, elle délimite le nombre d'assurés qui peuvent être assisté en même temps par une constante K. Ce coût existe donc si le nombre d'assurés infectés dépasse cette constante propre à l'assureur. Le coût de saturation s'écrit alors :

$$\mathrm{C}_2 = \mathbb{1}_{\sup t \mathrm{J}_t \geqslant K}$$

De la même manière que le coût ci-dessus, ce calcul repose sur la saturation probable de l'assureur. Si le cas se produit, alors des ressources supplémentaires entraînant une augmentation des coûts sont nécessaires pour que l'assureur réponde à ses engagements. On note alors t_d la durée de l'attaque et ϕ une fonction positive. Le coût de l'assistance de la proportion d'assurés infectés évolue en fonction de cette proportion. La fonction *phi* n'est pas linéaire, mais prend une forme particulière de telle manière qu'au-dessus d'un certain seuil, le coût de l'assureur explose. Ce coût prend donc la forme suivante afin d'être différent par unité de temps :

$$\mathrm{C}_3 = \int_0^{t_d} \phi(\frac{\mathrm{J}_t}{n}) dt$$

3.3.4 Modélisation du comportement et des variables de durées

On rappelle que :

— U est le temps nécessaire à un assuré pour être rétabli partiellement de l'attaque. Ce temps ne représente pas la durée pour laquelle l'assuré est complètement rétabli, mais dès que sa nécessité à être assisté par l'assureur n'est plus absolue. Elle peut donc être modélisée par une distribution exponentielle,

— C est la capacité de l'assuré à réagir à la crise. Elle reflète donc la rapidité à identifier l'attaque et à prévenir la DSI de l'entreprise. Cette action permet donc de mettre en place des mesures de prévention susceptibles d'éviter la diffusion de l'attaque à travers le portefeuille.

De cette manière, *C.Hillairet* et al. [9] établit 3 façons de modéliser la capacité C avec τ un délai de réaction comptabilisé en nombre de jours :

— avec une distribution exponentielle $\lambda_C^{(1)} = c_1 \mathbb{1}_{t \geqslant \tau_1}$ de telle façon que le comportement des assurés est indépendant du temps, il sera toujours le même au début de l'épidémie comme à la fin,

— avec une distribution de type pareto $\lambda_C^{(2)} = c_2(t - \tau_2 + 0,5)^{-\alpha_2} \mathbb{1}_{t \geqslant \tau_2}$ de telle façon que la vigilance des assurés diminue au fur et à mesure que l'épidémie progresse,

— avec une distribution de type weibull $\lambda_C^{(3)} = c_3(t - \tau_3)^{\alpha_3} \mathbb{1}_{t \geqslant \tau_3}$ de telle façon que la vigilance des assurés augmente au fur et à mesure que la propagation du virus progresse.

Cette modélisation permet de souligner deux points capitaux que l'assureur ne peut pas réellement contrôler lors de l'épidémie (mais lors de la souscription, la compagnie d'assurance peut essayer de convaincre l'entreprise de prendre certaines mesures vis-à-vis de ses employés) :

— le comportement des assurés a un rôle important dans la propagation du rançongiciel. Il peut, par lui-même ralentir ou accélérer le processus,

— sa réactivité à répondre à la crise est également un élément crucial dans la vitesse de propagation du rançongiciel.

3.4 Modélisation par graphe sous contrainte budgétaire

3.4.1 Contextualisation

Supposons qu'un graphe $G = (V, E, W)$ muni de n sommets et m arêtes avec un poids w_i sur chacune de ses arêtes où $i = \{1, .., m\}$ puisse représenter un portefeuille d'assurance exposé au risque de rançongiciel. Chaque assuré, ou pool d'assuré (où pool signifie un sous-portefeuille du portefeuille d'assurance global ayant de nombreuses caractéristiques identiques) peut être associé à un sommet du graphe G. Si une proximité existe entre deux sommets, autrement dit, s'il existe un lien entre deux assurés (ou pool d'assurés), tel qu'une proximité géographique, ou un secteur d'activités similaire, alors une arête relie ces deux sommets. Cette proximité est quantifiable par le poids de l'arête w_i. Plus la valeur de w_i est importante, plus les deux sommets seront proches. Enfin, si l'arête i et l'arête j (où $j = \{1, .., m\}$) partagent un sommet commun, alors ces deux arêtes sont considérées comme voisines.

3.4.1.1 Hypothèses et justifications du modèle épidémiologique

Afin de simuler la propagation d'un rançongiciel au sein du graphe G, il est nécessaire de définir les règles de modélisation. Cette Cyber-infection sera modélisée par un processus de réseau qui a

été présenté dans le chapitre 2. Les individus de la population exposée au rançongiciel sont donc les sommets qui peuvent être répartis dans les compartiments du modèle épidémiologique. Il serait tentant de reprendre le modèle SIR utilisé et développé précédemment, puisque comme justifié, il répond parfaitement à la propagation du *malware* étudié. Cependant, ses trois compartiments rendent l'analyse de la propagation du graphe difficile. En effet, il n'y a pas deux états possibles, mais trois. Il serait donc nécessaire de construire une variable aléatoire capable de représenter ces trois états tels qu'une variable aléatoire binomiale. Cependant, l'analyse de tous les changements d'état, l'obtention de cette information et la résolution d'un nombre exponentiel d'équations demeure un processus complexe. Il est donc plus judicieux de s'orienter vers un modèle épidémiologique constitué de deux états. Le modèle SI reste trop simple et trop inapproprié pour ce type de *malware*, tandis que le modèle susceptible-infecté-susceptible (SIS) peut mieux répondre à cette problématique. Même s'il a été montré que ce modèle ne décrivait pas la manière dont un rançongiciel se propage c'est-à-dire qu'un individu infecté ne puisse pas revenir sain.

Comme indiqué au début de cette sous-section, les sommets sont des assurés ou des pools d'assurés. En réalité, il n'y aura que des pools d'assurés. Ce choix de représentation permet donc de modifier la définition de l'individu. En effet, un individu pourra être représenté par un nombre d'assurés ayant des caractéristiques très similaires. Ainsi, lors de la propagation du rançongiciel, l'individu sera considéré comme infecté si une seule des entreprises de son pool est en réalité infectée. Bien que les probabilités que les autres soient également infectées à un instant proche, il est légitime de supposer que si le nombre d'entreprises composant le pool est assez grand, l'hypothèse qu'une entreprise soit infectée puis guérie alors qu'une entreprise du même pool demeure saine à un instant similaire demeure probable. Si l'on suppose également qu'un pool d'entreprises soit considéré comme infecté lorsqu'au moins une de ses entreprises est infectée et guérie lorsqu'aucune de ses entreprises n'est infectée, alors le modèle SIS devient logiquement adapté au processus de propagation des graphes.

3.4.1.2 Processus de diffusion par un modèle markovien dynamique

L'objectif de cette partie est de construire un modèle probabiliste particulier répondant aux hypothèses précédentes, autrement dit, celles du modèle SIS. Pour cela, il est nécessaire d'introduire un modèle markovien dynamique capable donc d'évoluer dans le temps.

Soit t, une variable désignant le temps, tel que $t \in [0, +\inf]$ et $X_i(t)$ une variable aléatoire de Bernouilli tel que :

$$X_i(t) = \begin{cases} 0 & \text{si l'arête } i \text{ est saine} \\ 1 & \text{si l'arête } i \text{ est infectée} \end{cases}$$

Ainsi, cette variable aléatoire de Bernouilli permet de décrire la dynamique des arêtes du graphe. En d'autres termes, deux options sont possibles à un instant t. Soit l'arête est considérée comme saine et $X_i(t) = 0$, soit elle est infectée et $X_i(t) = 1$. Cette valeur dépendante de t peut évoluer autant de fois que nécessaire. Afin de rester cohérent avec le modèle SIS décrit dans le chapitre 2, $X_i(t)$ peut évoluer selon deux critères :

— l'arête i est infectée, alors au bout d'un certain temps, elle redeviendra naturellement saine,
— l'arête i est saine et une de ses voisines est infectée, alors elle a une probabilité d'être infectée.

En réalité, ces changements d'états sont modélisés par des processus de Poisson. Lorsque $X_i(t) = 1$, l'arête i possède un taux de guérison noté λ_i qui est un processus de Poisson d'intensité λ_i. À l'inverse, lorsque $X_i(t) = 0$, l'arête i est dépendante de l'état de ses voisines et de l'intensité de leur connexion (i.e. w_i). Ainsi, pour chaque paire d'arête i et d'arête j avec $i \neq j$, il existe un processus de Poisson d'intensité B_{ij}. Il sera donc noté pour l'arête i, le taux d'infection valant $\sum_{j=1}^{m} \beta_{ij} a_{ij} X_j(t)$. Ainsi, le taux d'infection de l'arête i dépend de l'état de ses voisines $(X_j(t))$, de l'intensité de leur connexion

a_{ij} et du processus de Poisson β_{ij}

$X_i(t) : 0 \to 1$ avec les processus de Poisson suivants : $\sum_{j=1}^{m} \beta_{ij} a_{ij} X_j(t)$
$X_i(t) : 1 \to 0$ avec le processus de Poisson suivant : δ_i

Il reste à définir l'espace de probabilité sur lequel la propagation du rançongiciel va évoluée. Soit l'espace de probabilité $(\Omega, \mathcal{F}, \mathbb{P})$ doté d'une filtration $\mathbb{F} = (\mathcal{F}_t)_{t \geqslant 0}$ telle que la filtration soit continue à droite et que $\mathcal{F}_0$ contienne tous les ensembles $\mathbb{P}$-négligeable. $X_t = (X_1(t), ..., X_m(t)$ est un processus de Markov à temps continue ayant des càdlàg (continue à droite, limite à gauche) trajectoires dont l'espace des états est $E = \{0, 1\}^m$ et $X_0 = x \in E$. X est donc un processus de Feller, autrement dit, un processus de Markov en temps continu satisfaisant les conditions de régularité et associé à un générateur infinitésimal noté $\mathcal{G} : C(E) \to \mathbb{R}$ défini tel que :

$$Gf(x) = \sum_{i=1}^{m} \{(1 - x_i) \sum_{j=1}^{m} a_{ij} \beta_{ij} x_j + \delta_i x_i\} (f(x^i) - f(x)), x \in E, f \in C(E)$$

où $x_j^i = x_j$ pour $i \neq j$ et $x_j^i = 1 - x_i$. Les poids de la matrice d'adjacence sont a_{ij}. Enfin la famille $C(E)$ est constituée de toutes les fonctions sur E espace d'état.

Derrière le nom de générateur infinitésimal se trouve un outil mathématique permettant de probabiliser tous les changements d'états du processus de Markov à temps continue qui dans ce cas est de type saut pur. Par exemple, les matrices de transitions d'une chaine de Markov classique sont des générateurs infinitésimaux. Finalement, ce générateur infinitésimal permet d'obtenir une information sur le changement d'état de X_t, i.e, le moment où un $X_i(t)$ change de valeur.

Par ailleurs, l'espace des états noté E possède une cardinalité de 2^m puisque pour k arête d'infecté où $k \geqslant 0$, il existe $\binom{m}{k}$ combinaisons différentes. Ainsi, la cardinalité de E est équivalente à $\sum_{i=0}^{m} \binom{m}{i} = 2^m$.

Il est intéressant d'analyser la variation des $X_i(t)$ dans un court instant δt. Puisque $X_i(t + \Delta t)$ dépend de la valeur de $X_i(t)$ et que $X_i(t)$ dépendante du temps qu'une variable de Bernouilli qui évolue selon des processus de Poisson, il est possible d'écrire que :

$$\frac{X_i(t + \Delta t) + X_i(t)}{\Delta t} = (1 - X_i(t)) \sum_{j=1}^{m} \beta_{ij} a_{ij} X_j(t) - \delta_i X_i(t)$$

Les distributions à dimension finie de X sont donc analysables en résolvant un système d'équations différentielles ordinaires. Ainsi, en prenant l'espérance de l'égalité précédente et en faisant tendre Δt vers 0, l'équation suivante est obtenue :

$$\frac{\mathrm{d}\mathbb{E}[X_i(t)]}{dt} = \mathbb{E}[(1 - X_i(t)) \sum_{j=1}^{m} \beta_{ij} a_{ij} X_j(t) - \delta_i X_i(t)]$$

$$\Leftrightarrow \frac{\mathrm{dP}(X_i(t) = 1) \times 1 + \mathrm{P}(X_i(t) = 0) \times 0}{dt} = \sum_{j=1}^{m} \beta_{ij} a_{ij} \mathbb{E}[X_j(t)] - \sum_{j=1}^{m} \beta_{ij} a_{ij} \mathbb{E}[X_i(t) X_j(t)] - \delta_i \mathbb{E}[(X_i(t)]$$

En notant $v_i(t) = \mathrm{P}(X_i(t) = 1)$, on obtient pour chaque arête i du graphe l'équation suivante :

$$\frac{\mathrm{d}v_i(t)}{dt} = \sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t) - \sum_{j=1}^{m} \beta_{ij} a_{ij} \mathbb{E}[X_i(t) X_j(t)] - \delta_i v_i(t)$$

Conséquence directe des équations de Kolmogrov décrivant l'évolution temporelle de la probabilité que l'arête i soit infectée à un moment précis (qualifié de saut), les moments de X posent un réel problème. Ce système fini d'équations différentielles ordinaires d'ordre m contient $2^m - 1$ équations dû à $\mathbb{E}[X_i(t)X_j(t)]$ (qui nécessite de connaître l'évolution de tous les moments de X jusqu'au degré souhaité pour l'évaluation).Considéré comme fermé, ce système d'équation est donc impossible à résoudre. Numériquement, ce n'est pas le cas. *Van Mieghem et al.* [13] décrit la manière d'obtenir une solution dans sa section III intitulée *Exact* 2^N *state markov chain.* Cependant pour un nombre d'arêtes supérieur à 13, *Matthias Fahrenwaldt et al.* [7] a affirmé ne pas être capable d'obtenir une solution à ce système. Une solution pour contourner ce calcul est donc nécessaire et s'apparente sous la forme d'une méthode d'approximation des moments jusqu'à l'ordre n.

3.4.1.3 First order independant et First order Hilbert Mean field approximation

La méthode d'approximation des moments jusqu'à l'ordre n est totalement décrite dans le papier qui suit de *Matthias Fahrenwaldt et al.* [7] et s'intitule *N-Intertwined Mean Field Approximation.* Dans ce mémoire, seul les deux premières bornes du premier ordre seront décrites et détaillées.

Pour synthétiser, le système d'équations suivant pose problème, car il n'est pas analytiquement résolvable :

$$\frac{\mathrm{d}v_i(t)}{dt} = \sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t) - \sum_{j=1}^{m} \beta_{ij} a_{ij} \mathbb{E}[X_i(t) X_j(t)] - \delta_i v_i(t)$$

Les termes $\mathbb{E}[X_i(t)X_j(t)]$ pour $i \neq j$ ne sont pas directement calculables, puisqu'il nécessite de connaître la covariance des termes $X_i(t)$ et $X_j(t)$, autrement dit, les moments d'ordre supérieur (jusqu'à m). Au lieu d'augmenter le nombre d'équations jusqu'à $2^m - 1$ et être limité par la puissance de calcul, il a été admis qu'obtenir cette approximation au prix de l'exactitude est un choix pertinent.

Soit f, la fonction associée au calcul des termes du moment d'ordre 1 telle que :

$$\begin{array}{rccc} f & : & [\![0\ ;\ 1]\!] & \to & [0,1] \\ & & x & \mapsto & f(x) \end{array}$$

où $\mathbb{E}[X_i(t)X_j(t)] \approx f(\mathbb{E}[X_i(t)])f(\mathbb{E}[X_j(t)])$

Les fonctions $f(x) = \sqrt{x}$ et $f(x) = x$ sont les deux bornes encadrant les autres images de $f(\mathbb{E}[X_i(t)])f(\mathbb{E}[X_j(t)])$. La première borne pour $f(x) = \sqrt(x)$ est la borne inférieur. Cette approximation porte le nom de *First order Hilbert Mean field approximation.* La seconde borne pour $f(x) = x$ est la borne maximum s'intitulant *First order independent Mean field approximation.*

La raison pour laquelle ces deux fonctions encadrent les autres valeurs possibles est détaillée par *Matthias Fahrenwaldt et al.* [7]. Pour illustrer visuellement ces fonctions, considérons un graphe à 7 sommets dont la forme ainsi que la matrice d'adjacence sont :

$$A := \begin{pmatrix} 0&1&0&0&1&1&1 \\ 1&0&1&1&0&0&1 \\ 0&1&0&1&1&1&0 \\ 0&1&1&0&1&0&1 \\ 1&0&1&1&0&1&0 \\ 1&0&1&0&1&0&1 \\ 1&1&0&1&0&1&0 \end{pmatrix}$$

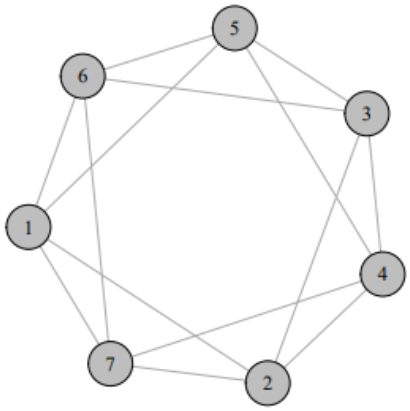

FIGURE 3.1 – Un graphe constitué de 7 sommets et 14 arêtes

En supposant qu'à l'instant $t = 0$, un rançongiciel s'auto-propageant se déclare sur le sommet 1, c'est à dire que le vecteur $v(0) = (v_1(0), .., v_7(0))^T = (1, 0, 0, 0, 0, 0, 0)^T$, il est alors possible de calculer la valeur des v_i selon les deux méthodes de calculs proposées ci-desssus (*First order Hilbert Mean field approximation* et *First order independent Mean field approximatio*).

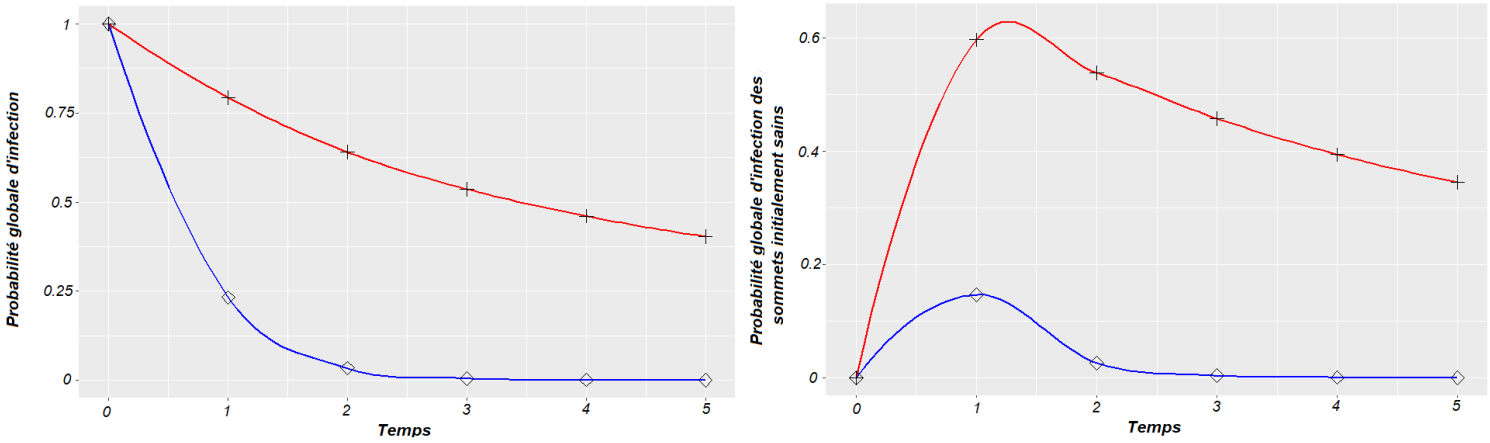

FIGURE 3.2 – Probabilité d'infection agrégée pour tous les sommets et pour tous les sommets sains

En rouge, la borne supérieure correspond à $f(x) = x$ et en bleu, la borne inférieure associée à $f(x) = \sqrt{x}$. La réelle courbe de ces valeurs se trouvent donc entre ces deux valeurs.

Le choix de la fonction f entre les deux bornes présentées ne demeure pas un choix crucial dans l'approximation des termes des moments d'ordre 1. Pour simplifier les calculs, il semble plus simple de choisir la borne de l'indépendance. De plus, ce choix est plus prudent puisqu'il reflète des probabilités d'infections plus importantes que la réalité. Cette supposition entraîne automatiquement que la corrélation de l'espérance des $X_i(t)$ soit nulle. Ainsi, il est possible de résoudre le système d'équation qui

s'apparenterait désormais pour chaque $i \in [\![1\ ;\ m]\!]$

$$\frac{\mathrm{d}v_i(t)}{dt} = \sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t) - \sum_{j=1}^{m} \beta_{ij} a_{ij} \mathbb{E}[X_i(t)]\mathbb{E}[X_j(t)] - \delta_i v_i(t)$$

$$\Leftrightarrow \frac{\mathrm{d}v_i(t)}{dt} = \sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t) - \sum_{j=1}^{m} \beta_{ij} a_{ij} v_i(t) v_j(t) - \delta_i v_i(t)$$

$$\Leftrightarrow \frac{\mathrm{d}v_i(t)}{dt} = (\sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t))(1 - v_i(t)) - \delta_i v_i(t)$$

En supposant que $\frac{\mathrm{d}v_i(t)}{dt} = 0$, il est possible d'obtenir la valeur à long terme du vecteur d'équilibre $(v_1(\infty), .., v_m(\infty)$ associé à l'équation précédente.

$$v_i(\infty) = \frac{\sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t))}{\delta_i + \sum_{j=1}^{m} \beta_{ij} a_{ij} v_j(t))}$$

Il existe deux solutions à cette équation. La première solution, la plus évidente, est celle du vecteur nul. Elle est appelée solution d'état stationnaire du modèle SIS. Cependant, une autre solution existe. Les conditions nécessaires à l'existence d'une telle solution sont démontrées par *N. Kazi-Tani et al.* [6]. Elle est appelée **état endémique** et est une solution non nulle de l'équation précédente.

3.4.1.4 Assurance et optimisation

Une des premières hypothèses formulée dans ce cadre là, est que l'assureur peut influencer directement sur le taux de guérison des arêtes. En effet, lorsqu'une Cyber-attaque se produit, les connexions touchées sont directement interrompues tant qu'elles sont considérées comme infectées. Elles mettent un certain temps (directement lié au taux de guérison δ_i) à ne plus être interrompues. Plus ce laps de temps est long, plus la sévérité du sinistre de l'entreprise est important. En effet, comme expliqué plus haut, l'assureur, en plus de payer le sinistre, s'engage à faire intervenir un expert en Cyber-sécurité ayant pour rôle de diminuer le temps d'interruption des activités de l'entreprise. De plus, la saturation des services de l'assureur lors d'une attaque massive de rançongiciel est un risque élevé. Ainsi, dans le cadre d'une saturation de ses services de type Cyber-sécurité, l'assureur devra choisir aléatoirement dans quelle entreprise elle souhaite envoyer ses experts de Cyber-sécurité.

Pour résumer, une entreprise touchée par un rançongiciel va voir le montant de son sinistre et le risque de contaminer d'autres entreprises augmenter. Ainsi, l'assureur a tout intérêt à essayer de cerner l'entreprise pour laquelle elle souhaite augmenter son taux de guérison δ_i, influençable par le taux d'assurance mise en place dans l'entreprise. Plus simplement, l'assureur se doit de cibler ce genre d'assurés.

Il semble également envisageable pour l'assureur de prévenir des entreprises qui pourraient avoir un rôle de super-contaminateur. Dans le même registre que précédemment, il est censé d'affirmer que l'assureur a la capacité de contrôler le taux de transmission de certaines entreprises. Lors de la souscription ou lorsqu'une épidémie se déclare, l'assureur peut demander à l'entreprise de respecter certaines conditions permettant la réduction de ce taux, comme la formation des employés à des mesures préventives, ou le renforcement de la Cyber-sécurité interne. De la même manière que pour le taux de guérison, si l'assureur choisit de manière réfléchie les entreprises dites super-contaminatrices, il peut contribuer à l'allégement de la propagation du rançongiciel. Ainsi, il est légitime de supposer que l'assureur peut également influencer directement sur le taux de transmission des assurés. Une

deuxième supposition est nécessaire pour pouvoir modéliser la première hypothèse. Désormais $\beta_i{=}\beta_{ij}$ $\forall j \in \{1,..,m\}$, c'est à dire que le taux de transmission ne dépend que de l'entreprise contaminée. En réalité, cette hypothèse n'est pas totalement absurde. La simplification de ce taux, est en partie absorbée par le poids affectés aux arêtes, représentatives de la proximité des entreprises.

Puisque ces mesures peuvent être prises par l'assureur, il serait intéressant de quantifier ces dernières. Supposons que lorsque l'état endémique arrive, l'interruption des différentes connexions engendre un sinistre noté Z_i (qui sont une séquence de variables aléatoires indépendantes et positives). Soit $\delta = (\delta_1, .., \delta_m)$ et $\beta = (\beta_1, .., \beta_m)$ les vecteurs de l'ensemble des taux de guérison et de transmission des infectés. Il sera alors désigné par $X(\delta)$ et $Y(\beta)$, les pertes totales des graphiques lorsque les vecteurs des taux δ et β sont ceux considérés sans l'intervention de l'assureur.

En passant par le principe d'espérance, il est possible d'obtenir la perte moyenne d'un graphe selon un vecteur d'un des taux :

— pour δ, la perte moyenne est notée $\mathbb{E}[X(\delta)]-\mathbb{E}[X(\delta^*)]$ où δ^* est le vecteur pour lequel l'assureur est intervenu. Plus l'écart est fort entre les δ et δ^* (où les δ^* sont supérieurs ou égaux aux δ), plus la perte moyenne diminue,
— pour β, la perte moyenne est notée $\mathbb{E}[X(\beta)] - \mathbb{E}[X(\beta^*)]$ où β^* est le vecteur pour lequel l'assureur est intervenu. Plus l'écart est fort entre les β et β^* (où les β^* sont inférieurs ou égales que les β), plus la perte moyenne diminue.

Les économies de l'assureur sont donc représentées par les deux fonctions suivantes :

$$c_1(\delta) = \mathbb{E}[X(\delta_0)] - \mathbb{E}[X(\delta)]$$

$$c_1(\beta) = \mathbb{E}[X(\beta_0)] - \mathbb{E}[X(\beta)]$$

Ainsi à la création de son portefeuille, l'assureur peut essayer de se questionner sur un problème d'optimisation lui permettant d'amoindrir les dégâts et la propagation.

Supposons que B représente le budget de l'assureur, il est possible de maximiser la connectivité du graphe, tout en minimisant les coûts évoqués. Le problème d'optimisation est donc le suivant :

$$\begin{array}{ll} \underset{\delta \in A}{\text{maximiser}} & \lambda_2(L) \\ \text{Sous contrainte de} & c(\delta) \leqslant B \end{array}$$

$$\begin{array}{ll} \underset{\delta \in A}{\text{maximiser}} & \lambda_2(L) \\ \text{Sous contrainte de} & c(\beta) \leqslant B \end{array}$$

Comme théorisée et démontrée par *N. Kazi-Tani et al.* [6], la résolution de problème non convexe, nécessite de reformuler la solution obtenue pour l'état endémique. Elle permet de reformuler l'équation, afin d'en déduire une représentation d'un β et d'un δ optimaux.

$$\delta_i^* = \left(\beta_i \sum_{j=1}^{m} a_{ij} v_i^*\right) \frac{1 - v_i^*}{v_i^*}$$

$$\beta_i^* = \left(\delta_i \sum_{j=1}^{m} a_{ij} v_i^*\right) \frac{1 - v_i^*}{v_i^*}$$

Ces deux éléments optimaux représentent une solution permettant à l'assureur de piloter sa gestion de l'épidémie en protégeant des assurés qui semblent être vecteur de l'infection informatique.

Pour conclure, cette section permet de continuer à théoriser (elle ne fera pas office d'application lors du chapitre 5) les travaux sur la théorie des graphes et les possibles applications et modernités qu'ils apportent. Conscient de sa difficulté à être mise en pratique, l'objectif est d'essayer de formuler des nouvelles visions et réponses au risque Cyber et particulièrement au risque de rançongiciel.

Chapitre 4

Bases de données, statistiques et calibrage

4.1 Les bases de données Cyber actuelles

Le problème majeur de la modélisation des risques dits Cyber est le manque cruel de données. Ce phénomène est dû en partie à la récente émergence du risque Cyber justifiant le peu d'historique disponible. Par ailleurs, les entreprises victimes de ce type de *malware* sont très réfractaires à l'idée de communiquer leur mésaventure, source d'une mauvaise image médiatique, d'une perte de confiance des clients, ainsi que d'une chute de leur cours boursier. Enfin, la difficulté à estimer la valeur d'une donnée et de la perte d'exploitation due à une impossibilité d'utiliser son parc informatique renforcent la mauvaise fiabilité des données récoltables. Ces éléments constituent donc la raison pour laquelle l'utilisation d'une base de données nécessaire à la calibration des paramètres des modèles semble compromise. Afin de justifier rigoureusement cette constatation, il paraît judicieux de reprendre les trois critères de la directive Solvabilité 2 sur la qualité de données et de les appliquer aux deux bases de données connues et gratuites du risque Cyber. Sur ces deux bases de données présentées, l'objectif est certes d'en déterminer la qualité, mais également de retrancher les informations concernant le risque de rançongiciel. Pour approfondir, il est conseillé de consulter les nombreuses littératures décrivant avec précision les données du risque Cyber dans un cadre général.

4.1.1 La base PRC

L'organisation à but non lucratif américaine *Privacy Rights Clearinghouse* (PRC) a pour conviction de responsabiliser les individus, de protéger leur vie privée et de plaider en faveur d'un changement positif dans le paysage de la confidentialité en constante évolution. C'est donc dans ce cadre que l'association a fusionné tous les incidents liés à la Cyber-sécurité afin d'en faire une base de données disponible et gratuite. Les évènements d'incidents relatifs au risque Cyber sont majoritairement obtenus auprès des procureurs généraux des États-Unis et du département américain de la Santé et des Services sociaux, mais également des médias et d'autres associations à but non lucratif. Néanmoins PRC signale que les données demeurent incomplètes en raison des différentes lois régissant certains états américains. On notera également l'absence du coût des sinistres. De plus, le jeu de données est en constante évolution et est consultable via le lien suivant : `https://privacyrights.org/data-breaches`. Dans ce mémoire, la base est téléchargée le 4 juin 2021 et compte 9015 sinistres. Cependant, les derniers sinistres ajoutés datent de 2019.

La base de données est facilement manipulable et interprétable. Elle est composée de 13 champs informatifs sur les incidents :

— *date Made Public* : année de déclaration de l'incident,
— *company* : entreprise victime de l'attaque,
— *city* : ville dans laquelle s'est déroulée le sinistre,
— *state* : état dans lequel s'est déroulé le sinistre,
— *type of Breach* : caractérise le type de violation causé par la Cyber-attaque. Elle peut être *HACK* (Piratage/Infection ou *malware*), *PHYS* (Physique), *PORT* (Appareil portable, smartphone), *STAT* (Perte d'ordinateur fixe), *DISC* (Divulgation involontaire n'impliqant pas de piratage), ou encore *UNKN* (Inconnu),
— *type of organization* : secteur d'activités de l'entreprise,
— *total Records* : nombre de DCP en jeu pour l'incident (Seul champ quantitatif),
— *description of incident* : description complète de l'attaque, informant de la procédure d'attaque et des éléments perdus par la victime,
— *information Source* : sources justifiant l'existence de cet incident,
— *source URL* : lien *HTML* redirigeant vers la source,
— *year of Breach* : année de survenance du sinistre,
— *latitude* : latitude du lieu du sinistre,
— *longitude* : longitude du lieu du sinistre,

De nombreux sinistres signalés ne correspondent pas à une attaque par rançongiciel. Le premier retranchement que l'on peut réaliser est de garder seulement les incidents dont le type de violation est causé par un *malware* (*HACK*). Le nombre de sinistres s'établit alors à 2533. Néanmoins, tous ces incidents ne sont pas forcément causés par un rançongiciel. Comme expliqué auparavant, il existe de nombreux types de *malwares* différents.

Le champ *Description of incident* peut contenir les informations du type exacte de *malwares*. Cependant, le terme *ransomware* n'est pas forcément utilisé et seul le principe du *malware* est décrit. Ainsi, pour regrouper tous ces évènements, le champ lexical du rançongiciel, avec une analyse des fréquences dans les articles anglophones décrivant ce phénomène s'avère pertinent. Le schéma suivant illustre les mots présents plus de 17 fois dans les premiers articles anglophones présentant les rançongiciels sur Internet. Pour information, les articles utilisés sont les suivants :

— `https://en.wikipedia.org/wiki/Ransomware`,
— `https://www.csoonline.com/article/3236183/what-is-ransomware-how-it-works-and-how-to-remo`
`html`,
— `https://www.cyber.gov.au/ransomware/examples-ransomware-incidents`,
— `https://www.ibm.com/downloads/cas/EV6NAQR4`.

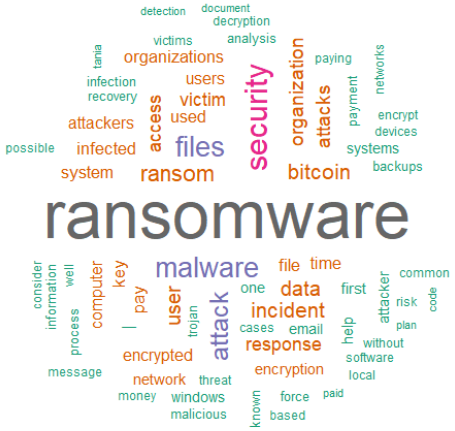

FIGURE 4.1 – Les mots liés au champ lexical du rançongiciel

Cependant, comme attendu, de nombreux mots sont propres au champ lexical du *malware*. C'est donc pourquoi il est judicieux de ne conserver que les mots caractérisant les rançongiciels de manière générale. La filtration des sinistres est réalisée selon les mots suivants :

- **ransom** : le terme de rançon est propre au phénomène de rançongiciel. Cela permet également de notifier les sinistres contenant des mots avec le préfixe *ransom*. 32 sinistres contiennent ce mot,
- **encrypt** : le processus de chiffrement est également unique au rançongiciel. 115 sinistres contiennent ce mot.
- ***Bitcoin*** : le paiement par cette cryptomonnaie est synonyme de rançongiciel. 5 sinistres contiennent ce mot,
- **pay** : le mot payer engendre généralement le rançongiciel. Il a été nécessaire d'enlever tous les mots dont le préfixe commence par *pay* afin d'éviter de retrouver les agissements sur les cartes de crédit (en anglais *credit card payment*). 44 sinistres contiennent ce mot,
- **crypto-currency** : toutes traces de cryptomonnaie sont fortement liées à un rançongiciel. 0 sinistre contient ce mot.

Une seconde piste pour retrouver les sinistres causés par un rançongiciel est de reproduire la procédure mais avec la liste des attaques de rançongiciel la plus connue : *WannaCry*, *Locky*, *Petya*, *CryptoLocker*, *Bad Rabbit*, *Jigsaw*, *Shade* et *Ryuk*. Seulement 1 sinistre contient dans sa description le rançongiciel *Shade*. De plus, cet incident avait déjà été révélé par les mots clés précédent.

Ainsi, la base comporte 174 sinistres qui pourraient répondre à un *malware* de type rançongiciel. Sur les 174 descriptions des sinistres, 155 ne contiennent qu'un seul mot du champs lexical, 16 contiennent 2 mots et 3 contiennent 3 mots. On peut désormais étudier la fréquence annuelle des sinistres par année de survenance :

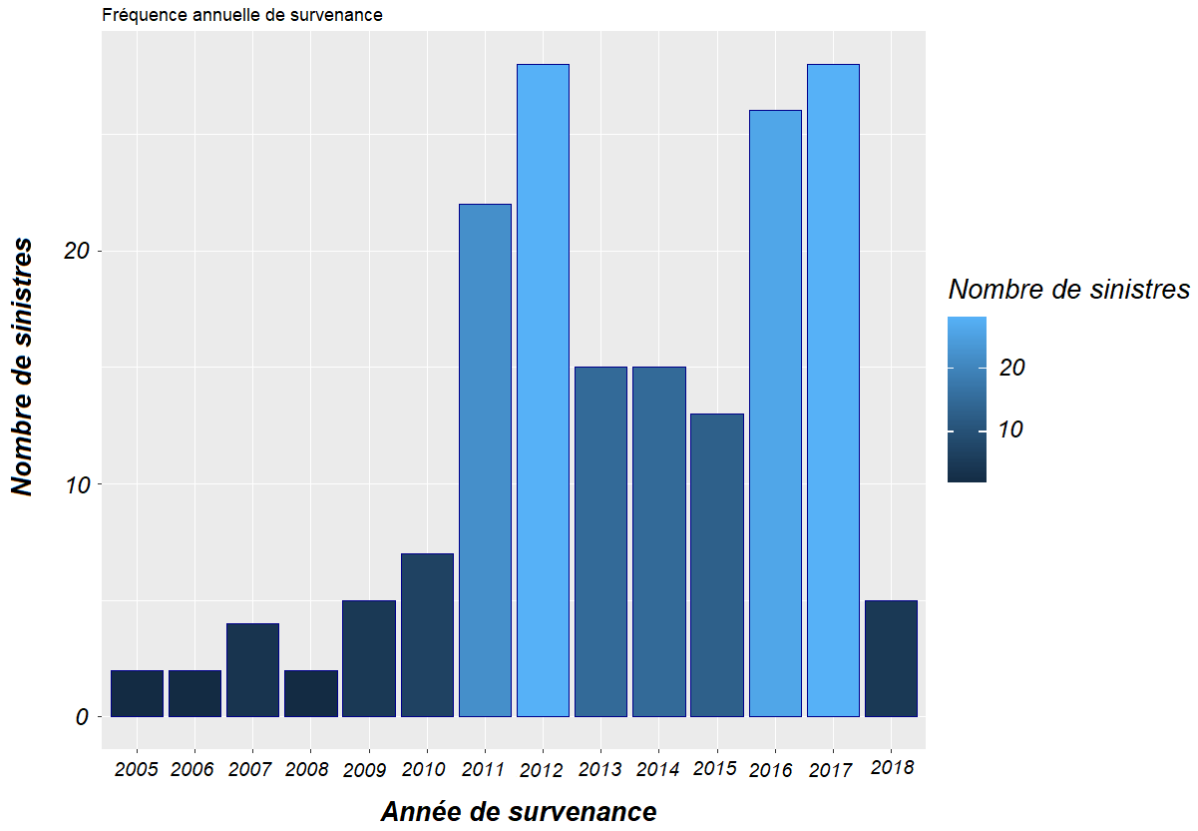

FIGURE 4.2 – Nombre de sinistres par année de survenance

L'année 2017 est très sinistrée (28 sinistres), ce qui est plutôt logique au regard des nombreux rançongiciels ayant sévis cette année. En ce qui concerne les années de survenance par rapport aux années de *reporting* (année à laquelle l'incident est déclaré et non survenu), tous les sinistres à l'exception d'un, sont déclarés à l'année de survenance. Enfin, un dernier champ peut être intéressant : le nombre de DCP. Dans le cadre d'un rançongiciel, le nombre de DCP est souvent élevé. En effet, si la rançon n'est pas payée, alors toutes les données du système informatique sont perdues. On a donc regroupé le nombre de DCP par groupe et on a observé le nombre de sinistres appartenant à ce groupe :

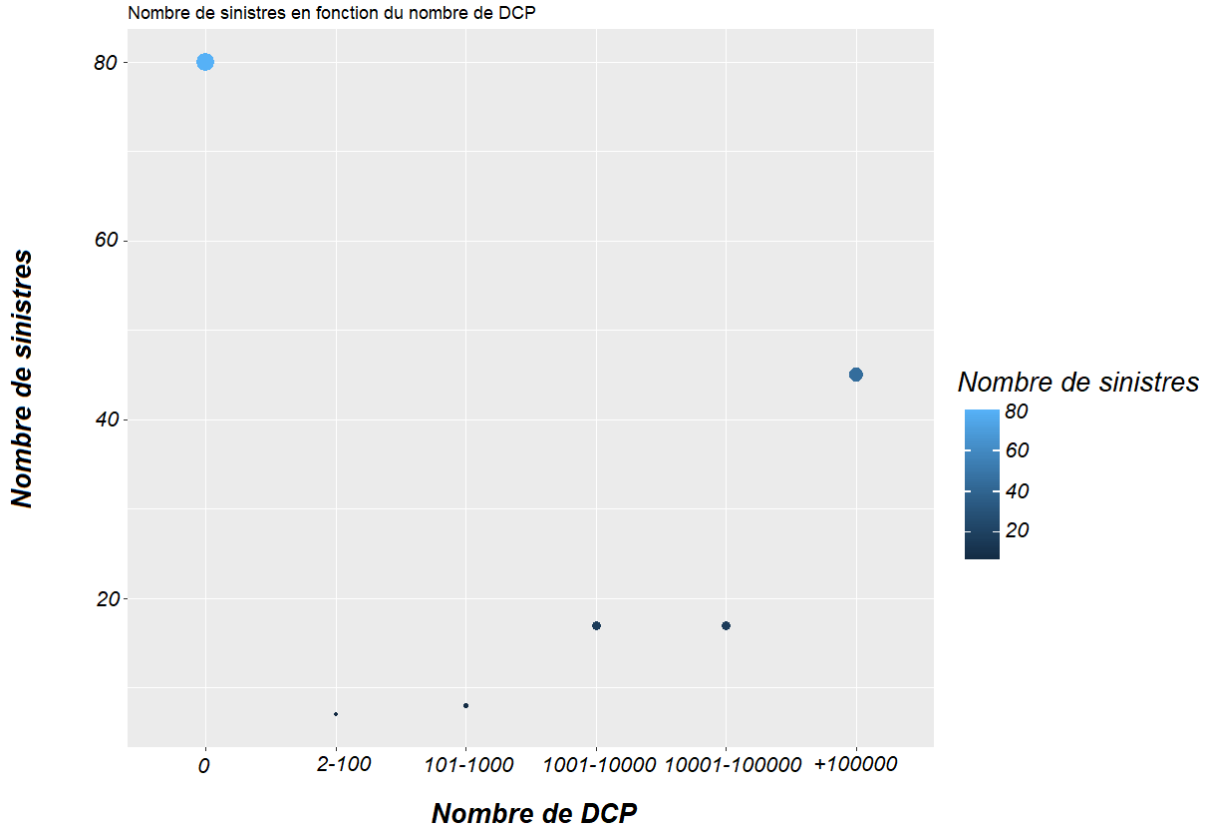

FIGURE 4.3 – Le nombre de sinistres selon les différents groupes du nombre de DCP

Le nombre de sinistres ayant 0 DCP peut signifier deux réalités. La première que la rançon du rançongiciel a été payée et que toutes les DCP ont été récupérées. Mais à la vue de la définition du champ *Total Records*, une seconde interprétation s'impose. Le nombre de DCP est celle en jeu pendant l'attaque. Dans ce cas-là, cela est sans doute dû à un manque d'information, puisqu'un rançongiciel chiffre l'entièreté des données. Il paraît donc incohérent d'affirmer qu'aucune DCP n'a été touchée.

Enfin, pour avoir une idée globale de la localisation de ses attaques, la figure suivante présente la longitude et la latitude de toutes les attaques par rançongiciel que la base de données recueille. Le jeu de données étant américain, il n'est en aucun cas surprenant d'observer une surreprésentation d'attaques aux États-unis.

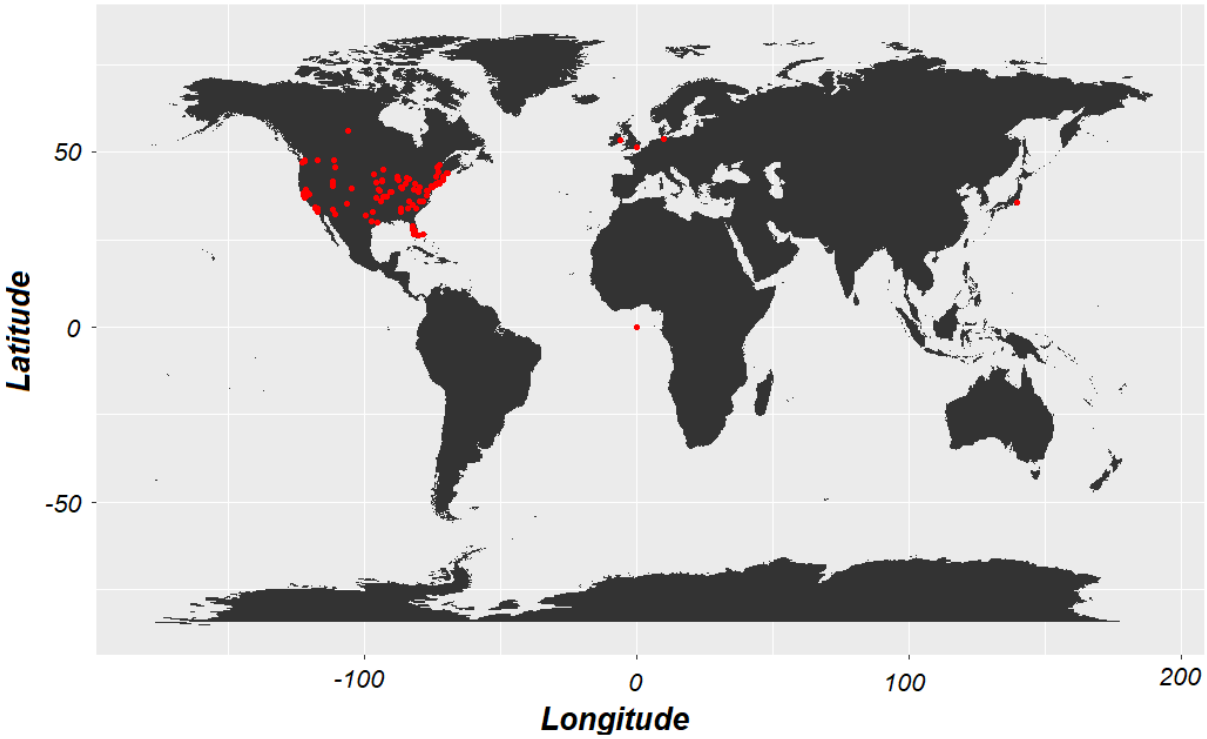

FIGURE 4.4 – Emplacement des différentes attaques de rançongiciel

Afin d'obtenir des informations sur la zone géographique des attaques aux États-Unis, les deux graphiques suivants proposent une analyse du nombre de DCP et des années de survenances selon les états américains.

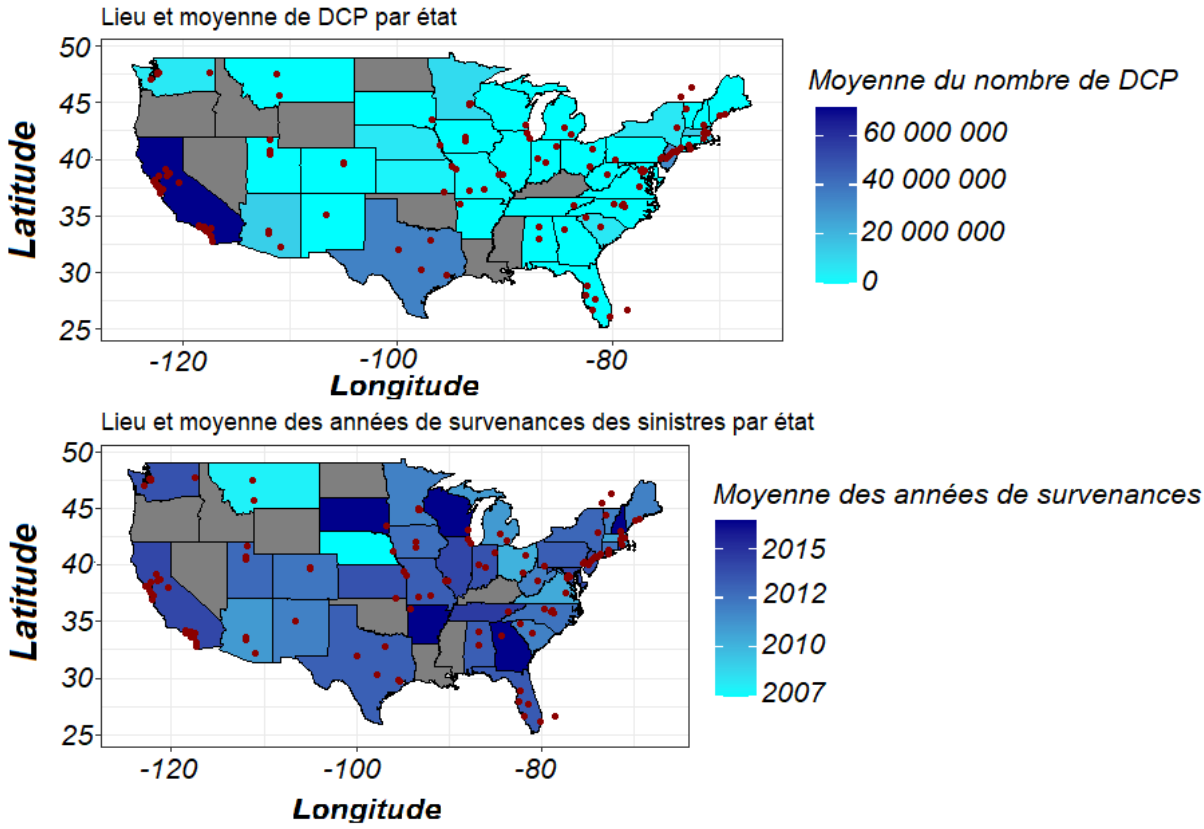

FIGURE 4.5 – Emplacements, DCP et survenances selon l'état américain

La Californie demeure comme l'état américain le plus attaqué et où le nombre de DCP perdues (calcul basé sur le nombre de DCP perdues par rapport au nombre d'attaques dans un état) est le plus important. L'explication la plus rationnelle à ce phénomène est sans doute la présence de la *Silicon Valley* en Californie, qui comporte de nombreuses entreprises dont les données sont sensibles. Le deuxième graphique permet d'observer un phénomène intéressant : les états (hormis la Californie) semblent subir des attaques dans une courte période. Par exemple, le Montana a connu deux attaques en 2007, alors que la Floride a été plus touchée par les rançongiciel au cours des années 2013, 2014. Il est donc possible de conclure que certaines zones sont sensibles à des attaques de rançongiciel selon des périodes données.

Finalement, ces deux graphiques permettent de faire l'hypothèse que la zone géographique peut être corrélée aux attaques par rançongiciel. L'écart de temps des attaques entre les entreprises situées dans la même zone géographique laisse imaginer que lfa proximité entre deux entreprises peut favoriser la propagation de l'attaque.

Pour conclure, la base PRC permet d'avoir une représentation globale des attaques par rançongiciel. Cependant, le manque d'historique et de sinistres empêchent de réaliser une analyse plus complexe des différentes variables du jeu de données.

4.1.2 La base VCDB

Alimentée depuis 2013, VCDB (*The Veris Community Database*) est une base collaboratrice ayant pour objectif de collecter tous les incidents liés au risque Cyber gratuitement. Le nom de VERIS (*The*

Vocabulary for Event Recording and Incident Sharing) ne correspond pas au jeu de données, mais à l'ensemble des métriques décrivant les incidents de sécurité de manière structurée et standardisée. Ainsi, chaque évènement survenu doit respecter un *reporting* spécifique permettant d'obtenir une qualité des données précise.

Deux sources alimentent ce jeu de données :

— un département étatique de l'administration américaine, le HHS (*Department of Health and Human Services*) qui est responsable de la politique en matière de santé,

— les SAG (*State Attorney General*) qui sont les procureurs généraux des 50 états américains.

La base de données est directement disponible sur le site de VERIS (`http://veriscommunity.net/`). Attention, le format des données est un *json* (*JavaScript Object Notation*). Cependant, il existe une version *csv* qui est utilisée dans ce mémoire. Pour information, la base de données a été téléchargée le 26 juin 2021 et comporte 8198 sinistres.

Contrairement à la base précédente, le nombre de champs informatifs peut sembler anormalement élevé puisqu'il existe 2441 champs différents. Cependant, ce nombre ne signifie pas qu'il demeure 2441 variables différentes. Afin de mieux comprendre le fonctionnement des colonnes, il semble judicieux d'expliquer la manière dont les champs informatifs ont été imaginés.

De nombreux champs sont en réalité des variables binaires permettant de catégoriser l'incident. Par exemple, pour connaître le pays où le sinistre a eu lieu, il existe autant de champs informatifs que de pays sur la terre, c'est à dire 249 possibilités différentes. Ainsi, pour chaque incident, seulement 1 des 249 champs apportera l'information sur la provenance du sinistre.

L'exemple précédent permet d'introduire le fonctionnement des champs informatifs de la base VCDB. 4 principales catégories sont utilisées pour détailler l'incident : *Actor, Action, Asset* et *Attribute*. Ces 4 macro-catégories sont également divisées en plusieurs sous catégories.

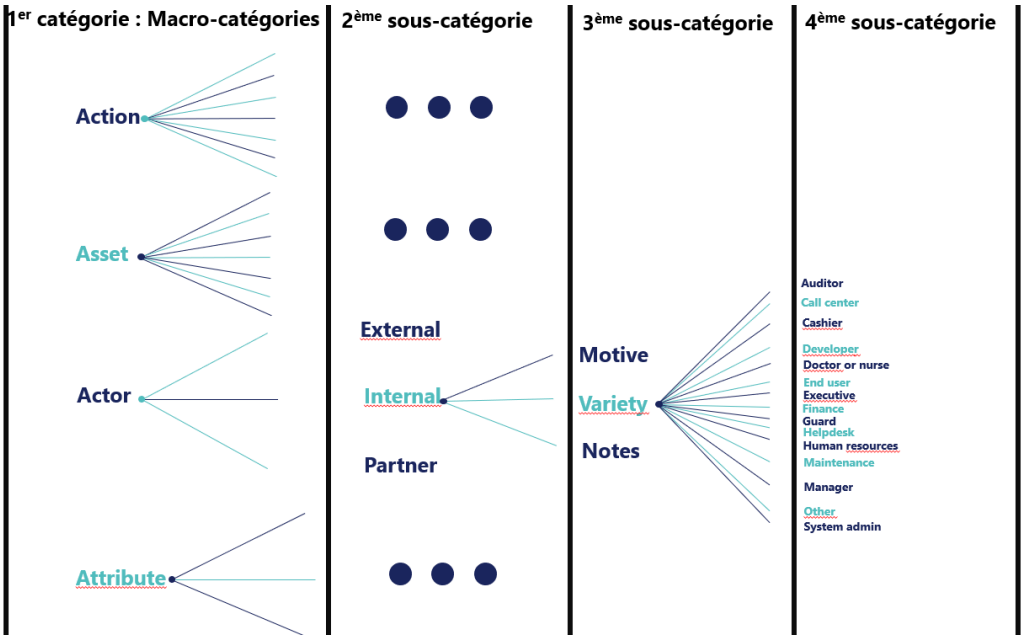

FIGURE 4.6 – Schéma simplifié du fonctionnement des champs informatifs de la base VCDB

Pour chacune de ces sous catégories, il existe encore d'autres catégories. Cela explique la façon dont fonctionne les champs informatifs de VCDB et le nombre élevé de colonnes. Certes, la base de données peut être aux premiers abords difficile à manipuler, mais cette manière de procéder garantit une qualité

concernant l'information des incidents. En réalité, le fonctionnement est un peu plus complexe : VERIS a introduit la notion de grille A^4 dont l'explication est disponible sur leur site.

Tous les champs informatifs ne seront donc pas cités puisque la majorité ne sont pas utilisés dans l'analyse proposée ici. Néanmoins, les champs retenus pour l'analyse de cette base de données sont listés ci-dessous :

— *country* : Pays touché par l'attaque,
— *year* : Année de survenance de l'attaque,
— *numberrecords* : Nombre de DCP en jeu lors de l'attaque,
— *sector* : secteur d'activités de l'entreprise attaquée,
— *lossUSD* : Coût des DCP perdues lors de l'attaques en dollar américain,
— *numberemployees* : Le nombre d'employés de l'entreprise attaquée,
— *trust* : Niveau de confiance des informations sur l'incident (*Low*, *Medium*, *High*, ou non déterminé).

De la même façon que pour la base PRC, de nombreux incidents présents ne coïncident pas avec une attaque par rançongiciel. Pour cela, il est possible d'utiliser le champs *action.malware.variety.Ransomware* donnant l'information si l'incident a été provoqué par le rançongiciel. Cette manipulation permet de retraiter la base de données et d'obtenir 165 sinistres. En exploitant le champs *action.malware.name*, il est possible de connaître le nom du malware responsable de l'incident. De manière semblable à la base PRC, l'utilisation d'une liste des rançongiciels connus permet d'obtenir quelques sinistres supplémentaires. En effet, le champs *action.malware.name* informe du nom du malware responsable de l'incident. En faisant concorder ces noms à la liste, il est possible d'obtenir 10 sinistres. En combinant les deux techniques de retraitement, notre nombre de sinistre évolue à 167. En effet, sur ces 10 sinistres, 2 n'était pas obtenus par la première technique.

Comme pour la base PRC, la première idée est de dégager une information de localisation. Cette base étant alimentée en grande partie par des entités américaines, il n'est en aucun cas surprenant d'observer une sur-représentation des attaques aux États-Unis. Afin de pallier cette prédominance, l'utilisation du logarithme sur le nombre d'attaques permet d'observer la tendance des incidents dans d'autres pays. La figure suivante présente donc une potentielle ébauche de la localisation des attaques :

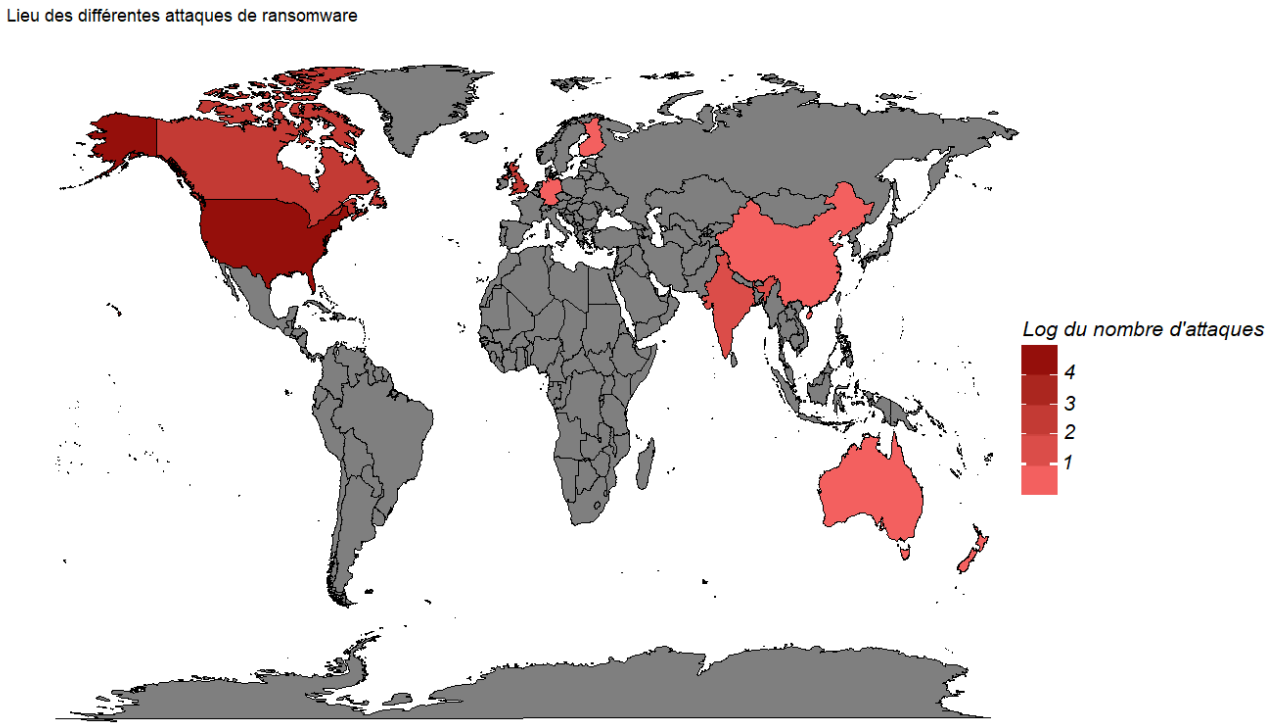

FIGURE 4.7 – Logarithme du nombre d'attaques dû à un rançongiciel par pays

La figure suivante permet d'observer les secteurs d'activités les plus sensibles aux attaques :

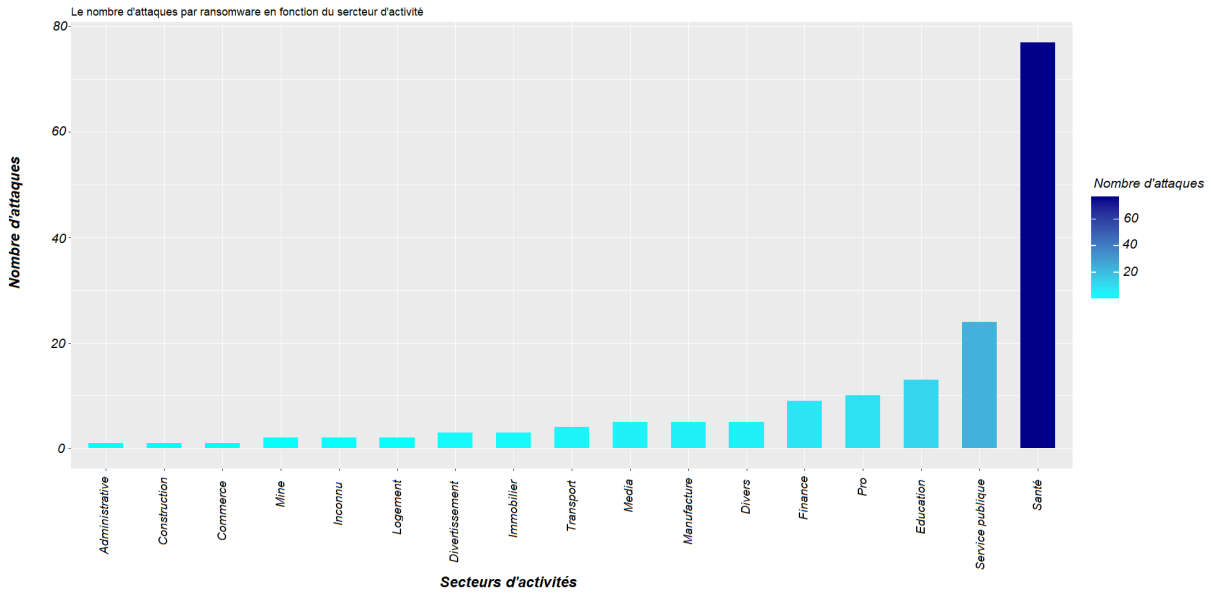

FIGURE 4.8 – Nombre d'attaques en fonction du secteur d'activités

Le domaine de la santé et du public ont été victimes de la moitié des incidents du jeu de données. En réalité, cette information est fortement biaisée par les sources alimentant la base VCDB. En

effet, comme mentionné précédemment, le HHS et les SAG signalent généralement des incidents qui demeurent dans leur domaine de prédilection, c'est à dire, la santé pour le HHS et le public pour les SAG. De plus, les institutions du publiques et de la santé ont tendance a plus facilement communiquer sur les attaques qu'elles peuvent subir comparé à certains secteurs d'activités du privé. Ainsi, le graphique précédent n'est pas totalement fidèle à la réalité. Néanmoins, il permet d'avoir une vision générale des domaines d'activité touchés.

En prenant le logarithme des coûts des DCP pour chaque secteur d'activités, il existe une forte disparité selon le secteur d'activités concerné comme en témoigne la figure suivante.

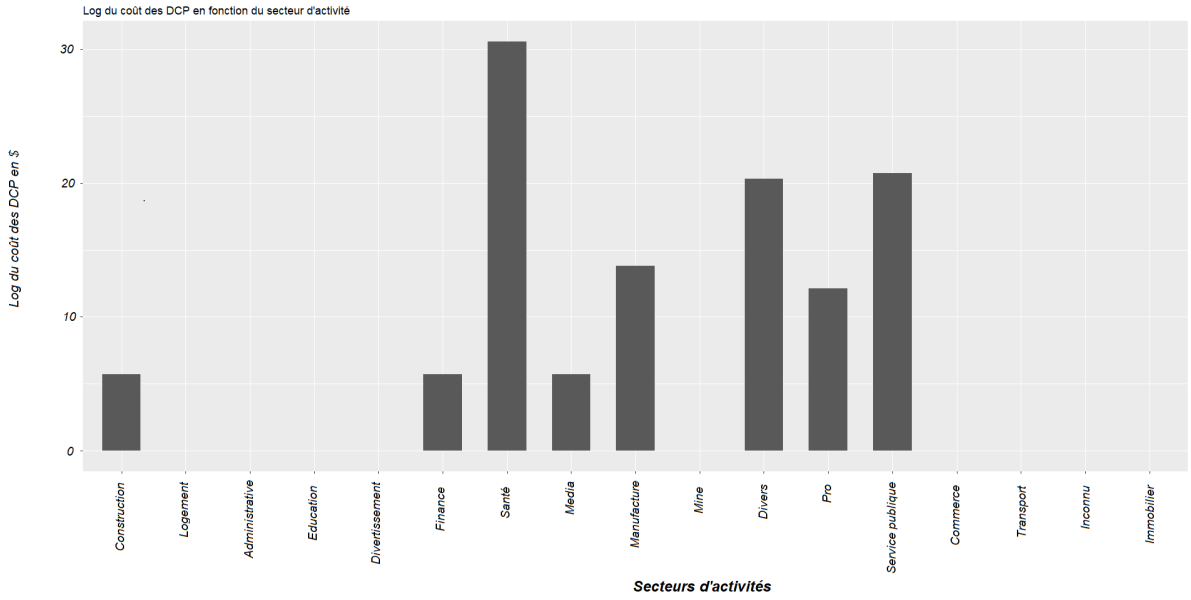

FIGURE 4.9 – Logarithme du coût des DCP en $ selon le secteur d'activités

Néanmoins, cela reflète le manque d'informations sur les sinistres provoqués par un rançongiciel. En effet, sur les 167 sinistres, seulement 14 fournissent le montant du coût des DCP en dollars. Finalement, le graphique précédent permet de conclure que de manière semblable à la base PRC, la base VERIS souffre du manque d'historique et de données. C'est donc pourquoi il est intéressant de regarder comment Solvabilité 2 approche le critère de qualité sur les bases de données utilisées par les assureurs.

4.2 Critère de qualité des bases de données

4.2.1 Succincts rappels des critères de qualité de données

Solvabilité 2 propose dans sa directive trois critères jaugeant la qualité d'une base de données. Cette initiative ne se réduit pas à une contrainte réglementaire. Elle a été pensée afin de limiter les risques liés aux travaux actuariels. En effet, des branches clés de l'actuariat sont fortement liées aux travaux sur les bases de données, comme la tarification, le provisionnement, ou encore la modélisation. Ainsi, ces trois éléments d'appréciation se doivent d'être soumis à la gouvernance de la fonction actuarielle. Un dispositif de gouvernance des données a donc été conçu et s'articule autour de six axes permettant d'encadrer la collecte de données et leur utilisation :

— principes d'organisation,
— dictionnaire de données,

— dispositif de contrôle,
— urbanisation et architecture du système d'information,
— processus de validation de la qualité des données,
— pilotage de la qualité des données.

Dans l'axe de processus de validation de la qualité des données et son pilotage, les trois critères au sens de Solvabilité 2 sont :

— **l'exhaustivité** : dans un premier temps, les groupes de risques homogènes doivent être identifiés par les données. De plus, afin de déterminer les tendances et l'évolution des risques sous-jacents, la granularité nécessite d'être suffisante (pour dissocier des risques en fonction de critères). Enfin l'historique des données est capitale,
— **l'exactitude** : elle définit que le cadre d'utilisation des données est approprié et adapté et que les données doivent refléter les risques auxquels l'assureur est exposé,
— **la pertinence** : ce critère désigne l'absence d'erreurs matérielles, la confiance portée aux données et une mise à jour fréquente de ces dernières.

4.2.2 Applications des critères de qualité aux bases Cyber

Afin de pouvoir juger la qualité des deux bases de données traitées ci-dessus, il est nécessaire de rappeler que ce jugement s'effectue seulement sur les sinistres dus à un rançongiciel. Pour un jugement général des bases de données, un tableau récapitulatif est disponible dans le mémoire de T.Bastard [2]. La figure suivante retrace le retraitement, ainsi que les avantages, les inconvénients, les biais et les défauts de deux jeux de données.

Avant/Après retraitement	Paramètre	PRC	VERIS
Base brute	Nombre d'incidents Nombre de champs	9015 13	8198 2441
Base retraitée	Nombre d'incidents Nombre de champs	174 13	167 7
	Nombre de variables quantitatives Nombre de variables qualitatives	1 12	3 4
	Nombre d'informations manquantes (en %)	3.24%	30%
	Champs de classification pertinent	1. Nombre de données perdues 2. Secteur d'activité	1. Nombre de données perdues 2. Nombre d'employés 3. Coût des données perdues 4. Secteur d'activité
	Biais et défauts de la base	- Américaine - Aucune information sur les coûts des sinistres - Trop peu d'incidents - Peu d'historique	- Américaine - Incidents fortement corrélés aux entités alimentant la base de donnée (Santé et public) - Trop peu d'incidents - Peu d'historique

FIGURE 4.10 – Récapitulatif des bases PRC et VCDB avant et après retraitement

Ce récapitulatif permet de procéder au jugement du critère de la qualité des données au sens de Solvabilité 2. Forcément, avec si peu de sinistres, des biais très marqués et des données manquantes, il est très difficile de se fier uniquement à ces bases pour construire un modèle viable. Ce qu'il faut donc retenir, c'est que la base PRC et la base VCDB constituent une excellente entrée en matière dans la compréhension du risque Cyber. Elles permettent d'avoir une vision plus étriquée des incidents dus aux rançongiciels, notamment sur la zone géographique et le secteur d'activités.

		Qualité des données PRC	Qualité des données VCDB
Exhaustivité	Identification de groupes à risque	Trop peu de données pour permettre l'identification des groupes à risques.	Malgré des champs plus précis, les groupes à risques sont difficilement identifiables.
	Granularité	Très peu de granularité.	Peu de granularité.
	Historique	Historique peu suffisant (2005 à 2019) et peu représentatif de la réalité.	Historique insuffisant et déséquilibrée (2007 à 2018), également peu représentatif de la réalité
Exactitude	Données adaptées au risque	Les biais de localisation (États-Unis) et de secteur d'activité desservent l'adaptation au risque. De plus, une seule variable est quantitative. Enfin, la source permet de vérifier l'exactitude des données.	Même problème que la base PRC, mais présence de plusieurs variables quantitatives. L'exactitude des données peut laisser à désirer.
	Reflète les risques d'un assureur	Absence du coût des sinistres empêchant une tarification de l'assureur.	Présence du coût des DCP, même si cette information demeure la seule en terme de coût. De plus, beaucoup de sinistres ne possèdent pas l'information (91%)
Pertinence	Absence d'erreurs	Malgré quelques incohérences, la présence de la source permet de compléter certains champs. Peu de données sont manquantes (3%)	Trop d'informations non communiquées (30%).
	Stockage adéquat de l'information	Les champs sont pertinents, et le fait que la base soit publique garantie ce point.	Les champs sont complets et pertinents. Le processus de la grille A^4 permet un excellent stockage de l'information
	Niveau de confiance	La source étant présente, les informations sont très souvent véridiques. Cependant les biais et le manque de données faussent ce point.	51% de *NA*, 5.4% de *Low*, 10% de *Medium* et 33.6% de *High* : Le niveau de confiance demeure léger, et les biais ainsi que le manque de de données faussent ce point.

Légende
Niveau de satisfaction
- Excellente
- Bonne
- Moyenne
- Médiocre
- Mauvaise

FIGURE 4.11 – Comparaison de la qualité des données selon de Solvabilité 2 pour la base PRC et VCDB

Pour conclure, les deux bases de données possèdent leurs propres avantages. Même si la base VCDB semble plus pertinente par son aspect de coût, en ce qui concerne les rançongiciels, les deux bases sont complémentaires et ne permettent pas à ce jour d'être la source d'un modèle de souscription, de tarification, ou de modélisation.

4.3 Complément de données aux bases actuelles

4.3.1 Les transactions *Bitcoin*

Ainsi que notifié précédemment, les paiements des derniers rançongiciels se font majoritairement par la cryptomonnaie du Bitcoin. Même si ces transactions demeurent presque intraçables, il est possible d'accéder à l'ensemble des paiements effectués. Afin de conserver l'anonymat, chaque détenteur de *Bitcoin* possède une adresse unique (et bien entendu indéchiffrable) redirigeant vers le compte du propriétaire. Cette adresse se présente sous format ASCII, ce qui signifie qu'elle est composée de lettres (à l'exception du i, I, o et O pour éviter les confusions) et de chiffres. Sans rentrer dans les détails des différents types d'adresses existantes, elles permettent donc de connaître le payeur et le receveur. Cette information peut être capitale dans l'obtention de données. En effet, lors d'une attaque massive de rançongiciel, les Cyber-criminels communiquent leur adresse *Bitcoin* afin de recevoir le paiement. Il est donc tout à fait possible de connaître à l'heure exacte, les transactions effectuées à une adresse précise.

En se rendant sur `blockchain.com/explorer`, l'accès aux transactions d'une adresse connue est possible. C'est ainsi qu'il existe sur `https://www.kaggle.com/shiheyingzhe/Bitcoin-transaction-data-from-2` toutes les transactions réalisées entre janvier 2009 et février 2018. Disponible au format *csv*,i.e. un format texte ouvert et malgré une volumétrie astronomique (53,06 gigaoctets), la consultation sous R demeure possible. Les différentes informations fournies par transactions sont les suivantes :

— **height** : c'est la hauteur du bloc appartenant à la blockchain. Pour résumer, c'est la position dans la chaîne d'un bloc qui lui-même est inscrit dans la blockchain. Cette information permet de connaître à quelle fréquence de nouveaux blocs sont minés (découverts). Pour rappel, la blockchain n'est pas infinie et est composée de 210 000 blocs,
— ***input*** : l'*input* correspond à l'adresse qui émet le paiement. En réalité, cette notion est un peu plus délicate. Chaque *input* correspond à un UTXO (*Unspend Transaction Output*). On peut assimiler un UTXO à un billet de banque. Chaque UTXO correspond à une somme précise et peut être utilisé pour le paiement. Ainsi si la somme de l'UTXO est inférieure à la somme du paiement, il faudra le compléter avec un autre UTXO. Il peut donc apparaître plusieurs *inputs* pour une seule transaction, mais cela ne désigne qu'une seule personne,
— ***output*** : l'*output* coïncide avec les adresses qui ont reçu le paiement. Comme l'UTXO dépasse généralement le paiement, plusieurs *outputs* peuvent être mentionnés. Un des *outputs* désigne l'adresse du receveur, tandis que l'autre renvoie vers l'adresse du payeur (différente de l'UTXO utilisé) qui reçoit son surplus. À noter que la somme totale payée ne correspond pas à la somme totale reçue. Une commission s'applique et est redistribuée au mineur des blocs,
— **sum** : c'est le montant total de la transaction en *Bitcoin*. Pour retrouver le prix en euro, il faut faire correspondre ce montant au cours du *Bitcoin* à la date du paiement,
— **time** : donne la date exacte à la seconde près de la transaction.

4.3.2 *Sophos* : État des ransomwares 2020

Créée en 1985 en Angleterre, *Sophos* est une entreprise dédiée à la création de logiciels de Cybersécurité. Elle a publié l'année dernière les résultats d'un sondage d'un cabinet de recherche indépendant *Vanson Bourne* ayant pour objectif de mieux comprendre le risque de rançongiciel et la manière dont les entreprises sont touchées. Il est possible de consulter entièrement le sondage en se rendant sur le lien suivant : `https://www.sophos.com/fr-fr/medialibrary/Gated-Assets/white-papers/sophos-the-state-of-ransomware-2020-wp.pdf`. Cette enquête a été réalisée auprès de 5000 DSI (directeur des systèmes d'information). Ces 5000 entreprises sont issues de 26 pays, où chaque nation comprend entre 100 et 500 répondants. Le secteur d'activités de ces entreprises est également varié, puisqu'aucun secteur d'activités n'excède 20% de la totalité des répondants.

Dans son étude, *Sophos* propose un résumé de l'étude permettant de mieux cerner les expériences des entreprises subissant une attaque par rançongiciel :

— 75% des attaques aboutissent au chiffrement des données,
— 94% des entreprises ont récupéré leurs données après paiement de la rançon,
— payer la rançon double le coût total du rançongiciel,
— contrairement aux idées reçues, le secteur privé est plus touché que celui du public,
— quand une entreprise est assurée et paye la rançon, l'assureur rembourse la rançon dans 94% des cas,
— alors que 84% des répondants possèdent une assurance Cyber, seulement 64% sont couverts contre le risque de rançongiciel,
— les États-unis ne sont que le 5ème pays le plus touché par les attaques de rançongiciel.

Ainsi, ce résumé démontre que les deux bases Cyber (PRC et VCDB) ne coïncident pas avec les informations que proposent l'enquête *Sophos*. Puisque la modélisation proposée dans ce mémoire repose grandement sur les secteurs d'activités, la zone géographique et la sévérité des sinistres, cette sous-section propose les 3 graphiques illustrant ces 3 phénomènes dans le cas d'une attaque par rançongiciel.

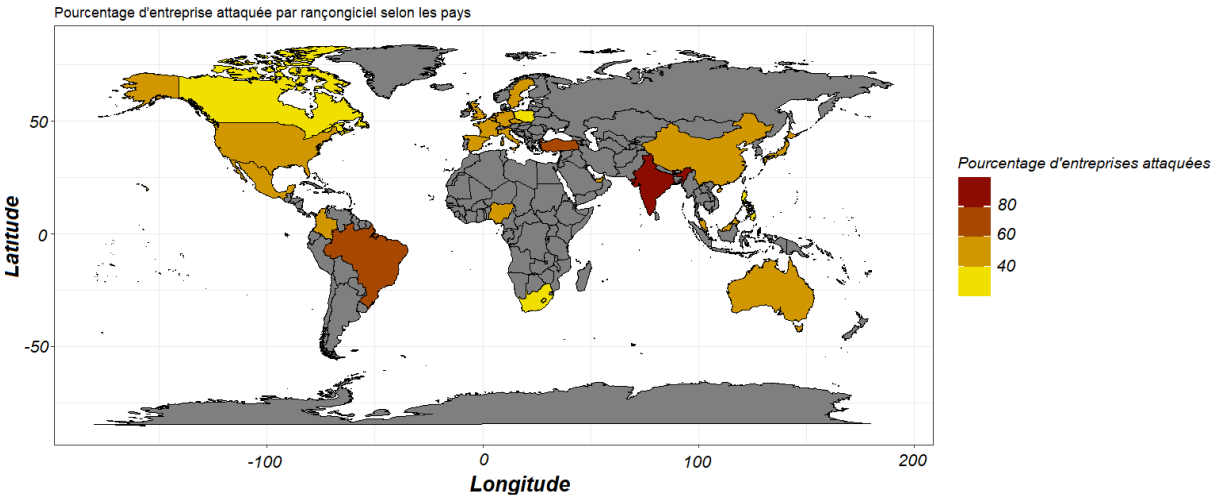

FIGURE 4.12 – Pourcentage des victimes touchées par un rançongiciel en fonction de la zone géographique (sur 5000 entreprises répondant au sondage)

Comme la figure précédente le montre, les pays les plus touchés sont en réalité les pays en émergence comme l'Inde ou le Brésil, tandis que les pays les plus développés (USA, Europe, Australie et Chine) subissent un nombre d'attaque équivalent. Le Canada fait résistance, puisque seulement 39% des entreprises sondées ont été frappées par un rançongiciel.

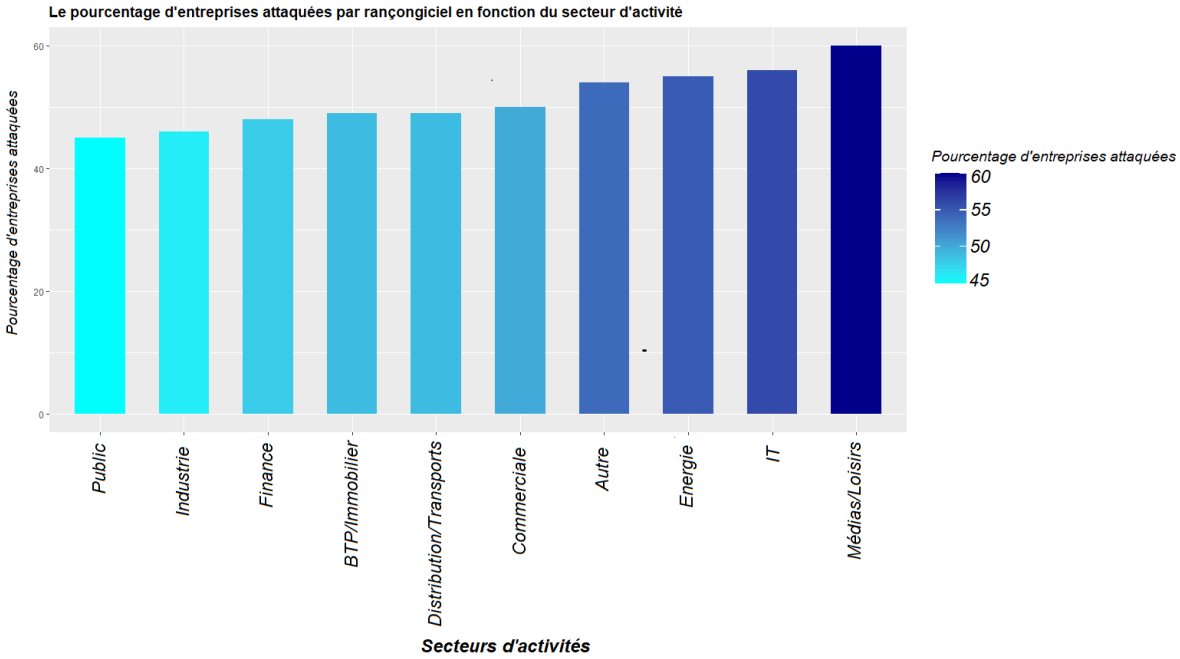

FIGURE 4.13 – Pourcentage des victimes touchées par un rançongiciel en fonction du secteur d'activités (sur 5000 entreprises répondant au sondage)

Même si le pourcentage d'entreprises touchées par un rançongiciel ne varie que très peu par secteur d'activités (15% de différence entre le plus et le moins sinistré), il est pertinent d'affirmer que le secteur public ne constitue pas la plus grande victime face à ce risque Cyber. De plus, *Sophos* relève un point

très pertinent : les entreprises étatiques sont obligées de déclarer toute attaque par rançongiciel alors que les entreprises du secteur privé ont tendance à ne pas le faire afin de ne pas subir une médiatisation trop forte engendrant généralement une mauvaise image marketing et économique. Ainsi, la réalité pourrait même être plus contrastée avec un secteur privé bien plus sinistré qu'il n'y parait.

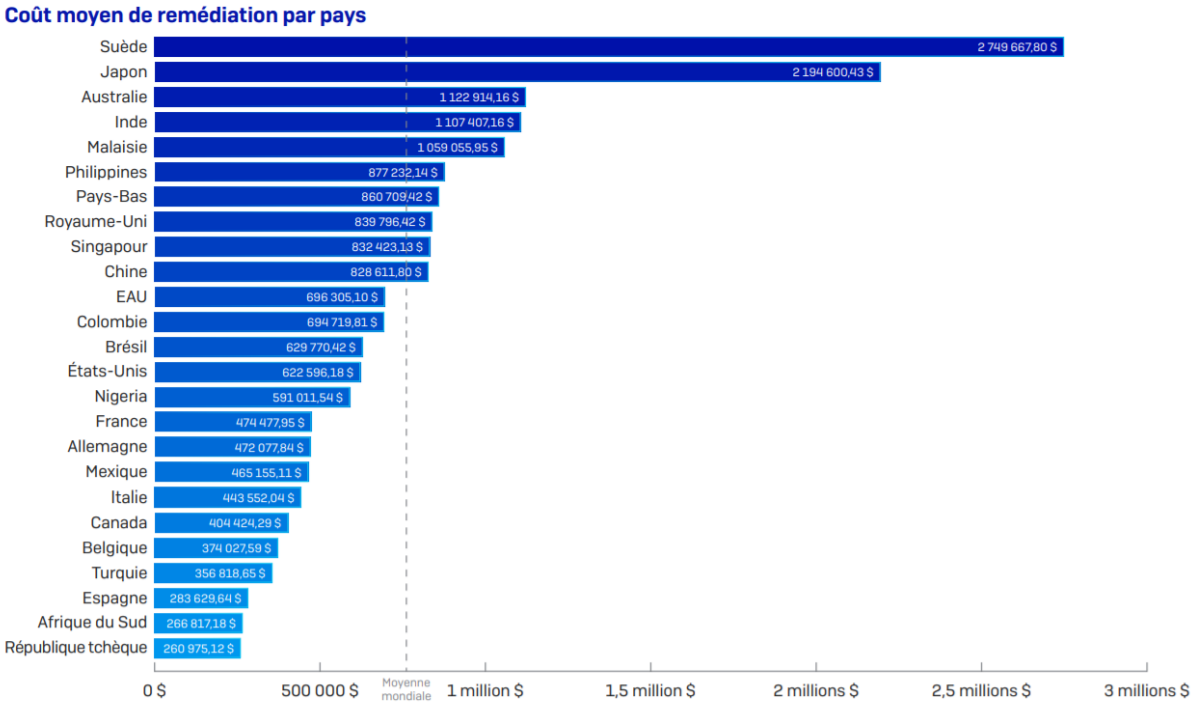

FIGURE 4.14 – Coût moyen d'une attaque par rançongiciel par zone géographique en dollars américains (sur 5000 entreprises répondant au sondage)

Le graphique précédent illustre que le coût des rançongiciel est très contrasté selon le pays dans laquelle l'entreprise évolue. Pour information, ces coûts comprennent les pannes, le temps de travail sacrifié, les coûts du matériel et du réseau, la perte d'exploitation, ainsi que la rançon à payer. La Suède et le Japon sont largement au-dessus de la moyenne. Selon *Sophos*, cela est en partie dû au niveau de salaire de ces pays, pour lesquels un arrêt de production engendre des coûts plus importants. Enfin, puisque payer la rançon double le coût du rançongiciel, les pays où les coûts moyens sont les plus élevés sont généralement ceux qui ont tendance à payer la rançon aux Cyber-criminels, toujours d'après *Sophos*.

4.3.3 Légitimité de ce type de données

Force est de constater que les données disponibles sur le risque d'attaque dû à un rançongiciel demeurent fragiles par leur manque d'historique et d'incidents. Les seules bases de données gratuites et exploitables paraissent en plus trop biaisées pour représenter une réalité que vient contraster le sondage de *Sophos*. L'objectif de ce chapitre est certes de montrer cette lacune, mais également de proposer une synthèse des données pouvant améliorer le "calibrage" des modèles actuariels. L'utilisation du terme "calibrer" peut s'avérer contestable à la vue des données présentées ci-dessus. Néanmoins, ces dernières permettent de nourrir les modèles imaginés avec des paramètres plus proches de la réalité.

Chapitre 5

Applications à l'assurance

5.1 Calibration

Dans un premier temps l'objectif de cette section est de justifier le choix des données qui vont permettre de calibrer les paramètres nécessaires à la réalisation des applications présentées dans ce mémoire. Pour rappel, les modèles présents ici doivent être alimentés et nourris par des données afin d'être fiables. Toutefois, l'objectif est de présenter des modèles dont le principe doit être assimilable aisément

De plus les paramètres à calibrer ne sont pas forcément propres au risque de rançongiciel, puisqu'ils doivent répondre à l'attente des modèles présentés dans les chapitres précédents ; et sont :

— le taux de transmission β, ainsi que le taux de guérison γ, donnant le R_0 similaire à des scénarios de type *WannaCry* ou *NotPetya*. Pour cela, il sera utilisé la base de données du *Bitcoin* présentée dans le chapitre précédent,
— différentes valeurs permettant de mieux représenter la *proximité* des différents secteurs d'activités, en fonction des pays, ainsi que plusieurs informations sur les secteurs d'activités les plus touchés, ou les mieux protégés. Cela permettra de calibrer les différents β de la matrice contenant tous les taux de transmission.

5.1.1 Choix des données

Ainsi qu'exposé lors du chapitre précédent, le manque de données du risque Cyber et en particulier du risque de rançongiciel s'auto-propageant, rend difficile la calibration des paramètres du modèle. Malgré le retraitement effectué, la taille et l'information des bases de données publiques PRC et VERIS ne permettent en aucun cas d'aider à la calibration des paramètres.

La calibration s'effectuera alors selon les sources suivantes :

— comme présenté lors du chapitre 4, l'historique de transactions du *Bitcoin* permet d'obtenir le nombre de paiements effectués pour l'épidémie d'un rançongiciel. A l'aide d'un proxy, c'est à dire une clé de répartition, il est possible d'obtenir une approximation du nombre d'entreprises infectées par la propagation d'un rançongiciel,
— même s'il ne s'agit que d'un sondage, l'étude de *Sophos* donne une vision plus précise et réelle du risque de rançongiciel selon les pays et les secteurs d'activités. Ces critères répondent parfaitement à la modélisation présentée et permettent également d'obtenir une information pertinente sur le coût,

— enfin, d'une façon similaire à *C.Hillairet* et al. [9], une des meilleures manières d'estimer la proximité des secteurs d'activités a été d'utiliser des informations comme la valeur ajoutée produite entre deux secteurs. Le site de l'*OCDE* (*Organisation de coopération et de développement économique*) présente des données utilisables. Il a été possible de télécharger les valeurs ajoutées produites entre des secteurs d'activités, ainsi que le nombre d'employés et le chiffre d'affaires.

5.1.2 Paramétrage du modèle épidémiologique : taux de transmission et taux de guérison

La base de données des transactions de *Bitcoin*, réalisées entre janvier 2009 et février 2018 et présentée dans le chapitre précédent, contient l'historique des paiements des entreprises infectées par des rançongiciels qui utilisent cette cryptomonnaie comme moyen de paiement. C'est le cas des deux plus célèbres *malwares*, *Wannacry* & *NotPetya*, présentés dans ce mémoire. En effet, lors de leurs attaques en 2017, ces virus informatiques ont communiqué des adresses *Bitcoin* afin de récolter les rançons. Ces informations sont facilement traçables sur internet et permettent de mieux cerner les épidémies des deux *malwares*. À titre informatif, les auteurs de *Wannacry* & *NotPetya* utilisaient les adresses *Bitcoin* suivantes :

— *13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94* (*Wannacry*),
— *12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw* (*Wannacry*),
— *115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn* (*Wannacry*),
— *1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX* (*NotPetya*).

Ainsi, la base de données contient le nombre de paiements quotidiens réalisé aux différentes adresses. Cela permet d'estimer le nombre d'entreprises infectées par jour en utilisant une règle de trois. De plus, il est également possible d'estimer ces informations par heure afin d'obtenir une courbe plus étalée dans le temps. Cependant, cela peut fausser l'estimation désirée puisque les rançons sont plus payées à certains créneaux horaires.

Les résultats obtenus sont les suivants :

— en 15 jours, 312 paiements ont été effectués auprès de *Wannacry*. En moyenne, cela représente 20,8 paiements par jour, avec un écart-type de 25,
— en 13 jours, 56 paiements ont été effectués auprès de *NotPetya*. En moyenne, cela représente 4 paiements par jour, avec un écart-type de 9.

La figure suivante permet d'observer la forme de la courbe des paiements de ces deux *malwares*.

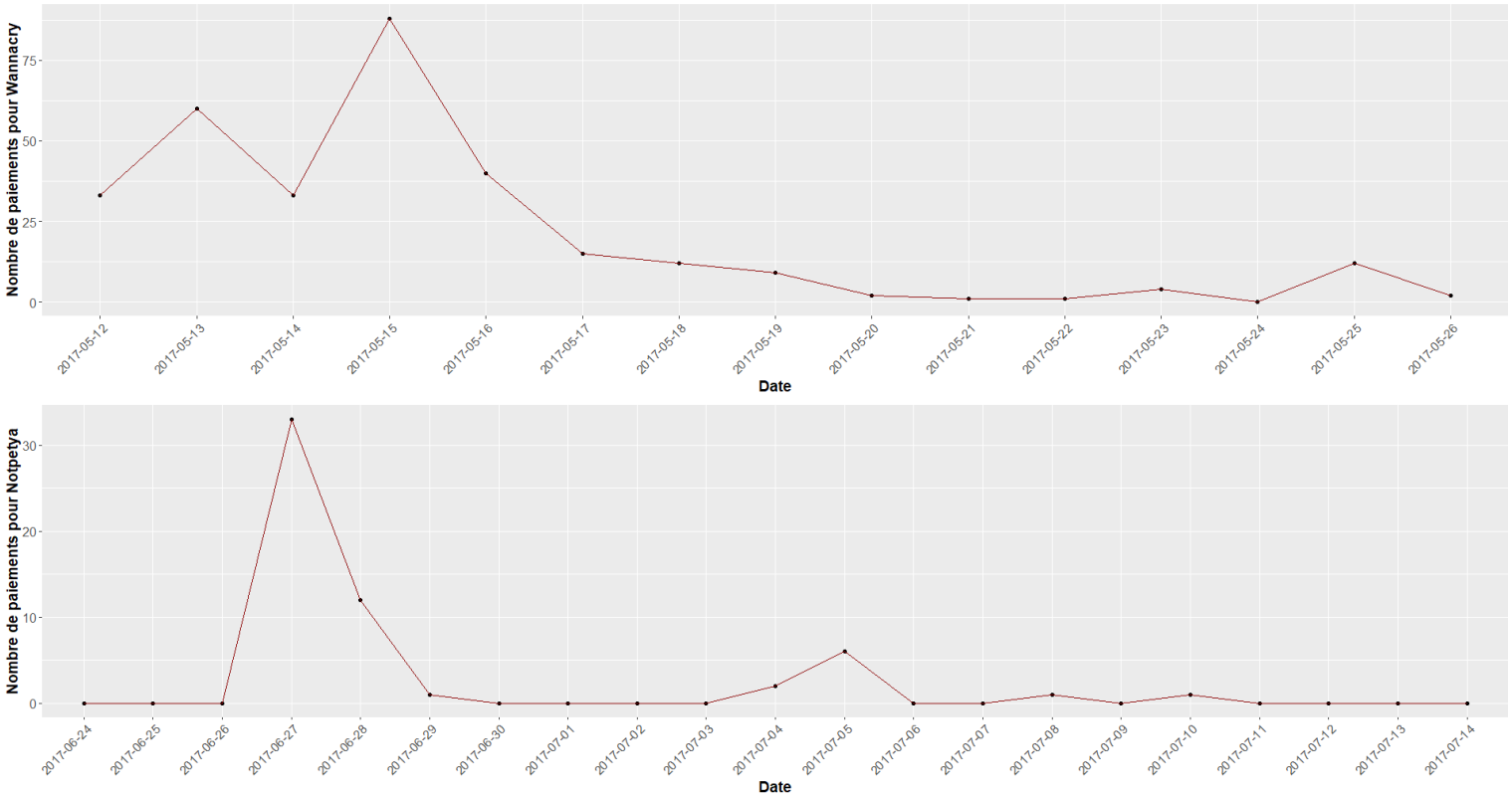

FIGURE 5.1 – Nombre de paiements par jour aux adresses *Bitcoin* des deux *malwares* concernés.

Même si l'approximation des paramètres du modèle épidémiologique demeure compliquée avec les éléments précédents, ces informations permettent d'apporter quelques notions pertinentes. Les deux courbes présentent plusieurs vagues confirmant que l'utilisation des modèles SIR multi-groupes sont plus réalistes. À la différence de *NotPetya*, il est possible d'observer une seconde vague plus intense que la première pour *Wannacry*. À la vue de cet élément et du nombre de paiements plus importants pour *Wannacry*, il semble plus intéressant d'essayer d'estimer les paramètres de ce *malware*, afin d'être dans la capacité de construire un scénario proche de ce qui a pu se passer en mai 2017.

Comme expliqué au cours de ce mémoire, la durée pendant laquelle l'entreprise infectée est contagieuse est plus courte que celle correspondant à sa cessation d'activité. Une entreprise sera contagieuse tant qu'elle n'aura pas pris conscience de son infection. Ainsi, même si l'activité n'a pas pleinement repris après plusieurs semaines, il sera considéré que l'entreprise sait qu'elle est infectée en moyenne au bout de 1 jour. Cependant, le but est de reproduire des scénarios identiques aux *malwares* présentés. De plus, il est également intéressant de faire varier ce paramètre en le probabilisant. Ce choix permettrait de démontrer à quel point la prise de conscience et la rapidité de réaction de l'entreprise peut réduire le risque de propagation. Finalement, pour l'estimation du taux de transmission, il sera noté que $\frac{1}{\gamma} =$ 1 jour.

Avec cette hypothèse, il reste à déterminer le taux de transmission β de l'épidémie qui donnera l'estimation du R_0. D'après Wikipédia et [8], *Wannacry* a fait plus de 300 000 victimes et la population totale exposée à ce risque était de 4 064 279. Ainsi, $N = 4064279$ et $R(\infty) = 1 - S(\infty) = 300000$ où $R(\infty)$ désigne le nombre d'entreprises guéries lorsque l'épidémie est terminée et $S(\infty)$ le nombre d'entreprises jamais infectées.

$$I_{max} = P_{max} \text{ x } \alpha = 93 \text{ x } 937,5 = 87188$$

Désormais, l'objectif est d'estimer le taux de transmission β. Le modèle SIR lie β et $r(\infty)$, puisque d'après le chapitre 2, l'équation suivante existe :

$$s(\infty) = s(0)\exp\left(-\frac{\beta}{\gamma}(1 - s(\infty))\right)$$

$$\Leftrightarrow r(\infty) = 1 - s(0)\exp\left(-\frac{\beta}{\gamma}(r(\infty))\right)$$

$$\Leftrightarrow \beta = \frac{-\gamma\log\left(1 - \frac{r(\infty)}{s(0)}\right)}{r(\infty)} = 1,04$$

Avec l'estimation du β, il est possible d'obtenir le R_0 qui vaut à peu près 1,04 grâce à l'équation suivante :

$$R_0 = \frac{\beta}{\gamma} = 1,04$$

La valeur du R_0 est relativement faible. Premièrement, elle est le résultat de nombreuses hypothèses. Dans un deuxième temps, "seulement" 7% de la population totale a été victime du rançongiciel.

Cette calibration a permis d'obtenir le taux de transmission β correspondant à un paramètre du modèle SIR simple. Cependant, pour l'application qui suit, il est nécessaire d'obtenir un β différent, qui s'appliquera à la matrice B contenant les proximités entre les secteurs d'activités. Plus clairement, la matrice B (détaillée dans la sous-section suivante, ainsi que dans l'annexe B) est le fruit de calcul de plusieurs indicateurs liés à l'estimation de la proximité des secteurs d'activités. Une fois la matrice B obtenue, le scalaire β la multiplie. Sa valeur régule alors l'ampleur de la propagation du rançongiciel. La valeur du β estimée précédemment n'est pas adaptée au modèle SIR multi-groupes. À épidémie équivalente, plus le nombre de groupes est important, plus la valeur du β doit diminuer. En effet, puisque les coefficients de la matrice B ne sont pas identiques, pour retrouver une épidémie équivalente, plusieurs tests ont été réalisés. Ces éléments seront détaillés par la suite.

Dans un objectif de réalisme, le taux de guérison γ ne sera pas constant, mais dynamique. En effet, pour chaque groupe du modèle SIR, le taux de guérison estimé sera différent. Ce changement a pour aspiration de modéliser le comportement des entreprises face à l'attaque d'un rançongiciel. Comme expliqué dans le chapitre 3, la rapidité à identifier l'attaque et à adopter le bon comportement peut influencer sur la durée de rétablissement (durée pendant laquelle l'entreprise est contagieuse). Ce point sera abordé dans la deuxième sous-section suivante.

5.1.3 Construction de la matrice B

Pour contextualiser à nouveau, la matrice B représente la proximité des secteurs d'activités. Autrement dit, le coefficient de la ligne i et de la colonne j représente le degré de proximité entre le secteur d'activités i et le secteur d'activités j. Une fois établi, un coefficient β plus faible que l'estimation précédente, est appliqué à la matrice afin d'obtenir une matrice B' telle que :

$$B' = \beta \times B$$

Chaque coefficient de la matrice B' représentera alors le sous-paramètre β_{ij} justifiant du taux de transmission entre le secteur d'activités i et le secteur d'activités j.

La valeur ajoutée produite par un secteur d'activités i pour le secteur d'activité j contribue à l'estimation de la proximité de ces deux secteurs d'activités. L'*OCDE* fournit ces indicateurs à tra-

vers une base de données disponible ici : `https://stats.oecd.org/BrandedView.aspx?oecd_bv_id=36ad4f20-en&doi=data-00827-en`. Pour rappel, la valeur ajoutée mesure la richesse brute créée. Ce jeu de données indique toutes les valeurs ajoutées créées par un secteur d'activités au profit de n'importe quel secteur d'activités.

Cet indicateur permet de ne mesurer qu'un échange de flux économique. L'hypothèse suivante est donc postulée : la proximité désirée est proportionnelle au flux économique des deux secteurs d'activités. Même s'il est difficile d'admettre cette hypothèse, elle demeure capitale dans la calibration de la matrice B.

Ensuite, une autre base de données fournie par L'*OCDE* est utilisée. Le lien suivant permet de la consulter : `https://stats.oecd.org/index.aspx?queryid=82736`. Ces nouvelles données offrent plusieurs indicateurs que ce soit par pays, par année et par secteur d'activités. En sélectionnant la même année que les valeurs ajoutées utilisées (2015), il est possible de fusionner ces différentes informations dans un objectif de calibration de la matrice B. Ces nouveaux indicateurs sont les suivants :

— le chiffre d'affaires (dans la monnaie du pays),
— le nombre d'entreprises.

Pour uniformiser le chiffre d'affaires dans une unité monétaire unique, un historique de 2015 des taux de différentes monnaies par rapport au dollar américain a été téléchargé depuis le site *Kaggle* (disponible ici : `https://www.kaggle.com/datasets/amin233/forex-top-currency-pairs-20002020`). Une moyenne pour chaque taux de change a été calculée sur l'année 2015, permettant d'appliquer ces derniers aux chiffres d'affaires correspondants. Finalement, tous ces chiffres d'affaires en dollar sont exprimés en euro.

Enfin, afin de mieux représenter la sécurité de chaque secteur d'activités face à un rançongiciel, deux informations du sondage *Sophos* ont été exploitées. La première se trouve être le pourcentage d'entreprises touchées par un rançongiciel au cours de l'année précédente. Le second correspond au pourcentage d'entreprises ayant une assurance couvrant dans ses garanties le risque de rançongiciel. Grâce à ces statistiques, il va être possible d'affiner la calibration de la matrice B.

L'application proposée dans la section suivante intitulée *Propagation d'un rançongiciel à travers trois portefeuilles* permet de choisir le nombre de secteurs d'activités concernés (autrement dit, la dimension de la matrice B). Dans les exemples proposés, tous les secteurs d'activités disponibles sont utilisés. La justification du choix de ces derniers est détaillée dans l'annexe B (*Application 1 : Rshiny et fonctionnement*).

La prochaine figure détaille les secteurs d'activités choisis, ainsi que l'évaluation de la proximité. L'obtention de cette matrice nécessite plusieurs étapes. Détaillées numériquement dans l'annexe B, les étapes sont résumées ci-dessous :

1. Comme justifié précédemment, chaque coefficient β_{ij} de la matrice B vaut la valeur ajoutée créée par le secteur d'activité i au profit du secteur d'activité j (c'est à dire VA_{ij}). Pour résumer $\beta_{ij} = \mathrm{VA}_{ij}$.
2. Un processus de symétrisation a été appliqué à la matrice. Autrement dit, l'hypothèse suivante est admise : le sens des flux économiques entre deux secteurs d'activités (les valeurs ajoutées créées) n'impacte pas la proximité entre ces deux secteurs. Seule la quantification de ces flux peut influencer cette proximité. Pour résumer $\beta_{ij} = \beta_{ji} = \frac{\mathrm{VA}_{ij}+\mathrm{VA}_{ji}}{2}$
3. Puisque des fortes valeurs ajoutées créées peuvent être dues à un nombre total d'entreprises élevé, tous les coefficients de la matrice B sont divisés par le nombre total d'entreprises présentes dans le secteur d'activités i et le secteur d'activités j (notée NT_{ij}). Pour résumer $\beta_{ij} = \frac{\mathrm{VA}_{ij}+\mathrm{VA}_{ji}}{2\mathrm{NT}_{ij}}$

4. Chaque β_{ij} est multiplié par le pourcentage d'entreprises des secteurs d'activités i et j touchés par un rançongiciel. En désignant L_i est le pourcentage d'entreprises du secteur d'activités i touchés par un rançongiciel, le coefficient est le suivant : $\beta_{ij} = \frac{\mathrm{VA}_{ij}+\mathrm{VA}_{ji}}{2\mathrm{NT}_{ij}} \times \frac{1+(L_i+L_j)}{2}$
5. Enfin, cette matrice a été normalisée, afin d'obtenir des valeurs comprises entre 0 et 1 (plus lisibles). Seul l'écart entre les valeurs permet de comparer les proximités estimées.

Au termes de ces étapes, la matrice représentant la contiguïté des secteurs d'activités est totalement estimée. Les valeurs, exprimées en pourcentage, sont disponibles sur la figure suivante.

	Mines et carrières	Fabrication	Electricité, gaz, eaux et déchets	Construction	Commerce de gros et de détail	Transport et stockage	Hébergement et restauration	Information et communication	Activités immobilières	Autres services
Mines et carrières	15,83%	1,47%	2,62%	0,46%	0,04%	0,33%	0,08%	0,11%	0,13%	0,02%
Fabrication	1,47%	11,93%	0,59%	0,96%	0,74%	0,69%	0,27%	0,42%	0,34%	0,42%
Electricité, gaz, eaux et déchets	2,62%	0,59%	14,43%	0,16%	0,06%	0,14%	0,07%	0,14%	0,19%	0,05%
Construction	0,46%	0,96%	0,16%	3,30%	0,23%	0,18%	0,04%	0,09%	0,15%	0,20%
Commerce de gros et de détail	0,04%	0,74%	0,06%	0,23%	1,79%	0,14%	0,10%	0,12%	0,14%	0,13%
Transport et stockage	0,33%	0,69%	0,14%	0,18%	0,14%	3,65%	0,07%	0,14%	0,12%	0,12%
Hébergement et restauration	0,08%	0,27%	0,07%	0,04%	0,10%	0,07%	2,05%	0,06%	0,12%	0,08%
Information et communication	0,11%	0,42%	0,14%	0,09%	0,12%	0,14%	0,06%	6,43%	0,19%	0,17%
Activités immobilières	0,13%	0,34%	0,19%	0,15%	0,14%	0,12%	0,12%	0,19%	13,15%	0,15%
Autres services	0,02%	0,42%	0,05%	0,20%	0,13%	0,12%	0,08%	0,17%	0,15%	0,95%

FIGURE 5.2 – Estimation en pourcentage de la matrice illustrant le degré de relation entre les différents secteurs d'activités. Lecture : Plus la valeur est grande, plus le degré de relation est important.

Ainsi expliqué lors du début de la sous-section, il reste à multiplier la matrice précédente par le scalaire représentant le taux de transmission β. Si la modélisation proposée était basée sur le modèle SIR simple, alors il serait possible d'utiliser le β estimé grâce à l'historique du *Bitcoin*. Cependant, l'emploi du modèle multi-groupes empêche de recourir à l'estimation obtenue du taux de transmission. Comme énoncé dans cette sous-section, appliquer ce taux à plusieurs groupes n'a pas le même impact qu'un seul groupe. Si l'on garde le même taux pour la matrice, l'épidémie modélisée sera totalement différente par rapport à ce qui est souhaité. Cela explique donc pourquoi le β proposé lors des simulations sera différent de celui utilisé pour l'estimation. Plusieurs valeurs doivent être utilisées selon le nombre de secteurs d'activités pris en compte dans la simulation.

5.1.4 Estimation du taux de guérison γ

Pour rendre l'estimation du R_0 plus simple, le taux de guérison a été fixé à 1 jour. Néanmoins pour que la simulation soit plus dynamique et plus sensibles aux différents secteurs d'activités, la calibration du γ est légèrement modifiée. Pour information, plus le taux est élevé, plus le R_0 diminuera.

Comme mentionné dans la section 4, les statistiques issues de *Sophos* fournissent le pourcentage d'entreprises possédant une assurance couvrant dans ses garanties le risque de rançongiciel par secteur d'activités. L'hypothèse est donc la suivante : plus ce pourcentage est élevé (i.e. plus le secteur d'activités est couvert), plus le taux de guérison γ est haut (i.e. plus sa durée de rétablissement est supposée courte). Une seconde hypothèse est formulée : le temps de réaction d'une entreprise infectée

est aléatoire face à ce genre d'évènement. La couverture du risque par l'entreprise est proportionnelle à son temps de réaction. Ces hypothèses sont fondées sur 2 points. Premièrement, les entreprises couvertes sont conscientes du risque. Deuxièmement, elles sont accompagnées par l'assureur et peuvent avoir accès à une assistance gratuite et rapide.

Pour modéliser ce phénomène, le taux de guérison γ est différent pour chaque secteur d'activités et sa calibration résulte d'une loi de probabilité. Pour chaque secteur d'activité, le paramètre des lois de probabilités n'est pas identique, car il dépend du pourcentage d'entreprises couvertes face à ce risque par secteur d'activités. 3 lois sont ainsi proposées pour illustrer différentes réactions et comportements des entreprises infectées :

— une loi exponentielle de paramètre $\lambda = 2,48 - 2g_i$ où g_i est le pourcentage d'entreprises couvertes face au risque pour le secteur d'activité i,

— une loi de Weibull de paramètre fixe $k = 2,5$ et $\lambda = 0,38 + g_i$ où g_i est le pourcentage d'entreprises couvertes face au risque pour le secteur d'activité i,

— une loi log-normale de paramètre fixe $\sigma = 0,55$ et $\mu = \log(1,38g_i)$ où g_i est le pourcentage d'entreprises couvertes face au risque pour le secteur d'activité i.

Le paramètre γ dans le modèle SIR est très sensible. En effet, ce paramètre peut avoir un impact très important sur la durée de l'épidémie, puisque son inverse représente la durée de rétablissement (et donc d'infection). Ainsi, si la valeur du γ est très petite (et donc la durée de l'infection longue), alors l'épidémie sera généralement plus virulente. Les lois utilisées sont donc bornées afin de ne pas simuler des scénarios d'épidémie trop extrêmes. Au mieux, les bornes de γ sont 0,5 pour la valeur minimum et 1,15 pour la valeur maximum. Dans le cas du minimum, cela représente une durée de 2 jours où l'entreprise peut contaminer et ne réagit pas.

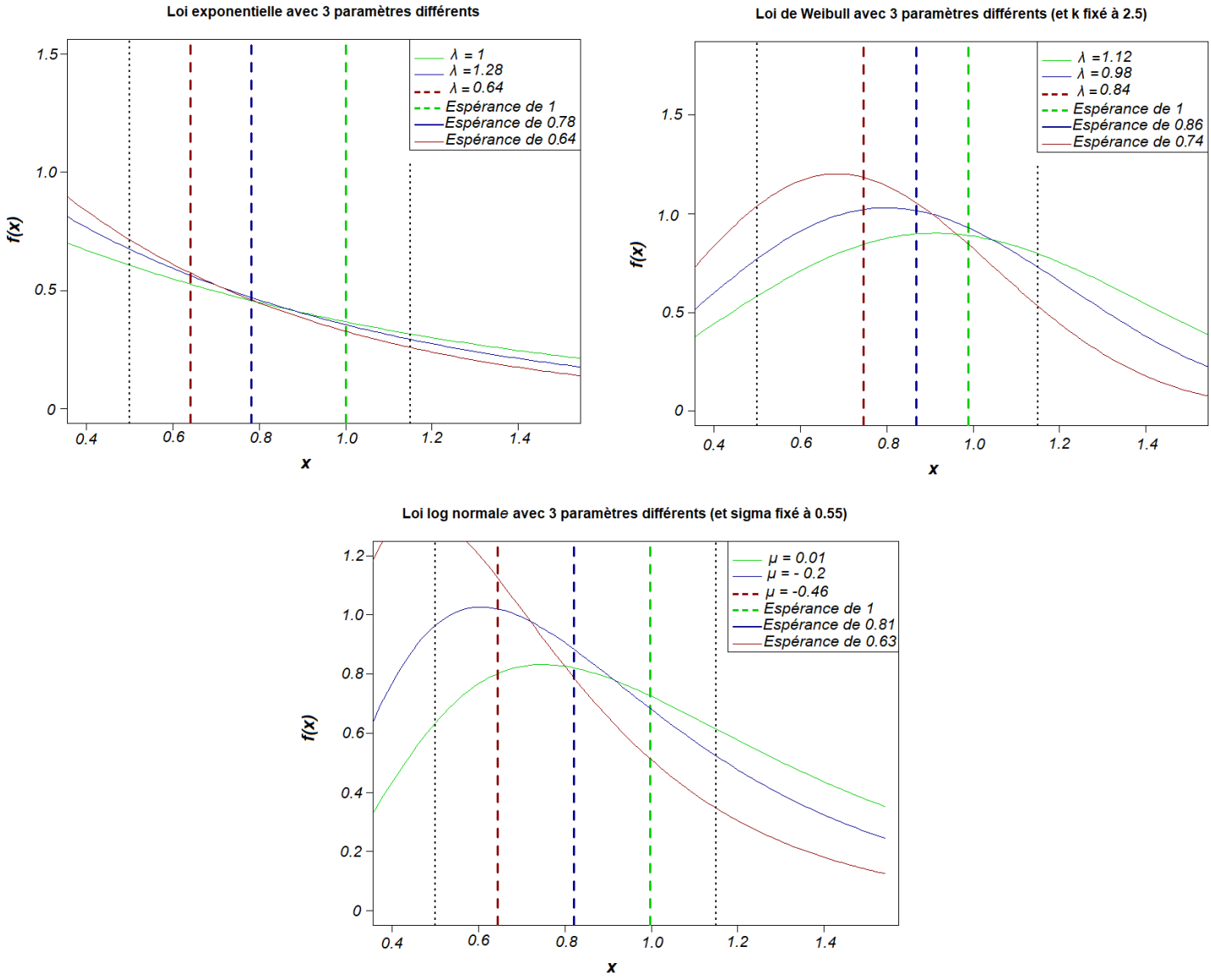

FIGURE 5.3 – Les densités de probabilités des 3 lois utilisées pour modéliser le taux de guérison γ. Le pourcentage (estimé) maximum d'entreprises couvertes face au risque donne une espérance de 1 jour. Les lois sont bornées entre 0,5 et 1,15.

La calibration des paramètres des lois a été choisie afin de respecter deux critères :

— puisque selon le sondage *Sophos* 75% est le pourcentage du secteur d'activité où les entreprises sont le mieux couvertes face au risque de rançongiciel, l'espérance des lois choisies vaut 1 jour,
— les autres pourcentages représentent donc le maximum et le minimum de la statistique utilisée. Elles ne sont pas les mêmes, mais sont dans des proportions similaires.

Chacune de ces lois modélisent une réaction différente des entreprises lorsqu'elles deviennent infectées similairement aux travaux présentés lors du chapitre 3 de *C.Hillairet* et al. [9]. Un autre phénomène représenté est la non-linéarité du paramétrage (à l'exception de la loi de Weibull). Autrement dit, plus le pourcentage est élevé, plus il aura un impact positif : le gain n'est donc pas linéaire. (Pour rappel, plus le taux de guérison est bas, plus la durée de guérison est haute).

— loi exponentielle : la réaction est lente, peu d'entreprises agissent rapidement. Plus le temps passe, plus les entreprises commencent à prendre connaissance de l'attaque.

— loi de Weibull : la réaction est presque de type "*normale*". Le nombre d'entreprises réagissant vite est équivalent au nombre d'entreprises réagissant lentement. L'espérance correspond donc à la plus grande majorité des comportements,

— loi log-normale : cette loi est similaire à la loi exponentielle. Toutefois, elle permet de diminuer le nombre d'entreprises ayant des comportements trop lents ce qui peut envenimer l'épidémie.

5.1.5 Estimation du coût

Le montant des sinistres Cyber, et particulièrement ceux du rançongiciel, sont difficiles à estimer. Toujours dû au manque de données et à la récente augmentation de sa sévérité (observé sur l'augmentation des ratios S/P en 2021 chez les assureurs), l'estimation demeure une étape délicate. Étant dans l'incapacité de proposer une estimation du coût d'un rançongiciel basée sur les bases de données présentées dans le mémoire, le coût a été construit de la façon suivante :

Dans un premier temps, un *coût secteur* est défini. Comme son nom l'indique, ce dernier est propre à chaque secteur d'activités. Il s'agit du rapport du chiffre d'affaires total du secteur voulu par rapport à son nombre d'entreprises. Ce résultat est ensuite divisé par la moyenne des rapports de tous les secteurs d'activités. Cela permet d'obtenir un écart par rapport à la moyenne, qui est donc de 1. Plus précisément, pour chaque secteur d'activités i, la formule est la suivante :

$$(\text{Coût secteur})_i = \frac{\frac{(\text{Total chiffre d'affaires})_i}{\text{Nombre d'entreprises})_i}}{\text{mean}(\frac{(\text{Total chiffre d'affaires})}{\text{Nombre d'entreprises})}}$$

À titre d'illustration, ci-dessous la valeur des différents coûts estimés :

secteur d'activités	**Valeur du coût**
Mines et carrières	0,4528309
Fabrication	2,9831527
Électricité, gaz, eaux et déchets	4,0324563
Construction	0,3950985
Commerce de gros et de détail	0,7886527
Transport et stockage	0,1148833
Hébergement et restauration	0,2156351
Information et communication	0,5687617
Activités immobilières	0,2818712
Autres services	0,1666575

Ces valeurs représentent un facteur du coût selon le secteur d'activités. En cas de perte d'exploitation (activité stoppée ou partielle), elles permettent uniquement de distinguer les secteurs d'activités où le coût final risque d'être plus important.

Pour estimer le coût d'un rançongiciel, la statistique de l'étude réalisée par *Sophos* a été utilisée. Pour chaque pays présent dans l'étude, *Sophos* a communiqué le coût moyen de remédiation après avoir subi une attaque par rançongiciel. En multipliant ces coûts par les facteurs des coûts secteurs, il est obtenu, pour chaque pays et chaque secteur d'activités, une valeur unique (après conversion en euro, puisque le sondage est en dollars). La prochaine figure illustre la valeur et la variation des coûts estimés.

	Mines et carrières	Fabrication	Électricité, gaz, eaux et déchets	Construction	Commerce de gros et de détail	Transport et stockage	Hébergement et restauration	Information et communication	Activités immobilières	Autres services	Moyenne
Australie	462 726	3 048 340	4 120 573	403 732	805 886	117 394	220 347	581 190	288 031	170 299	**1 021 852**
Belgique	154 128	1 015 361	1 372 507	134 478	268 430	39 102	73 395	193 587	95 939	56 724	**340 365**
Canada	166 654	1 097 878	1 484 049	145 407	290 245	42 280	79 359	209 319	103 736	61 334	**368 026**
République Tchéque	107 542	708 461	957 658	93 831	187 295	27 283	51 211	135 074	66 941	39 579	**237 487**
France	195 521	1 288 050	1 741 113	170 594	340 520	49 604	93 106	245 577	121 705	71 959	**431 775**
Allemagne	194 532	1 281 535	1 732 306	169 731	338 798	49 353	92 635	244 335	121 089	71 595	**429 591**
Italie	182 777	1 204 097	1 627 630	159 475	318 326	46 371	87 037	229 571	113 772	67 268	**403 632**
Japon	904 342	5 957 614	8 053 164	789 046	1 575 008	229 432	430 642	1 135 866	562 921	332 829	**1 997 086**
Pays-bas	354 678	2 336 541	3 158 404	309 459	617 709	89 982	168 895	445 480	220 774	130 534	**783 246**
Pologne	321 564	2 118 395	2 863 526	280 567	560 038	81 581	153 127	403 889	200 162	118 347	**710 119**
Espagne	116 877	769 961	1 040 789	101 976	203 554	29 652	55 656	146 799	72 752	43 015	**258 103**
Suède	1 133 072	7 464 438	10 090 003	988 615	1 973 365	287 461	539 562	1 423 154	705 297	417 010	**2 502 198**
Turquie	147 036	968 645	1 309 359	128 290	256 079	37 303	70 018	184 680	91 525	54 115	**324 705**
Royaume-Uni	346 060	2 279 769	3 081 662	301 940	602 700	87 796	164 792	434 656	215 410	127 362	**764 215**
USA	256 557	1 690 142	2 284 639	223 848	446 821	65 089	122 171	322 239	159 698	94 422	**566 562**
Moyenne	**336 271**	**2 215 282**	**2 994 492**	**293 399**	**585 652**	**85 312**	**160 130**	**422 361**	**209 317**	**123 759**	742 598

FIGURE 5.4 – Coût moyen estimé en euro de remédiation d'une entreprise suite à un sinistre de rançongiciel par pays et par secteur d'activités.

La figure précédente permet de mettre en avant les disparités des coûts estimés. Par exemple, les sociétés d'électricité, de gaz, d'eaux et de déchets en Suède ou au Japon ont des coûts complètement différents des entreprises de transport ou de stockage en République tchéque.

5.2 Propagation d'un rançongiciel à travers trois portefeuilles

5.2.1 Application Rshiny

La particularité de cette application est que les lecteurs peuvent l'utiliser. Développer en R sous *Rstudio*, le code est disponible sur le GitHub suivant : `https://github.com/GeoffreyBard/Cyber-Ransomware-Model`. Le fonctionnement de l'application est détaillé en annexe B.

À l'aide de Rshiny, un package de R permettant de développer des GUI (*Graphical User Interface*), l'application permet de facilement modifier les paramètres du modèle, la composition d'un portefeuille ainsi que quelques options supplémentaires. Une fois que les paramètres sont sélectionnés, un bouton permet de lancer l'application détaillée dans cette section.

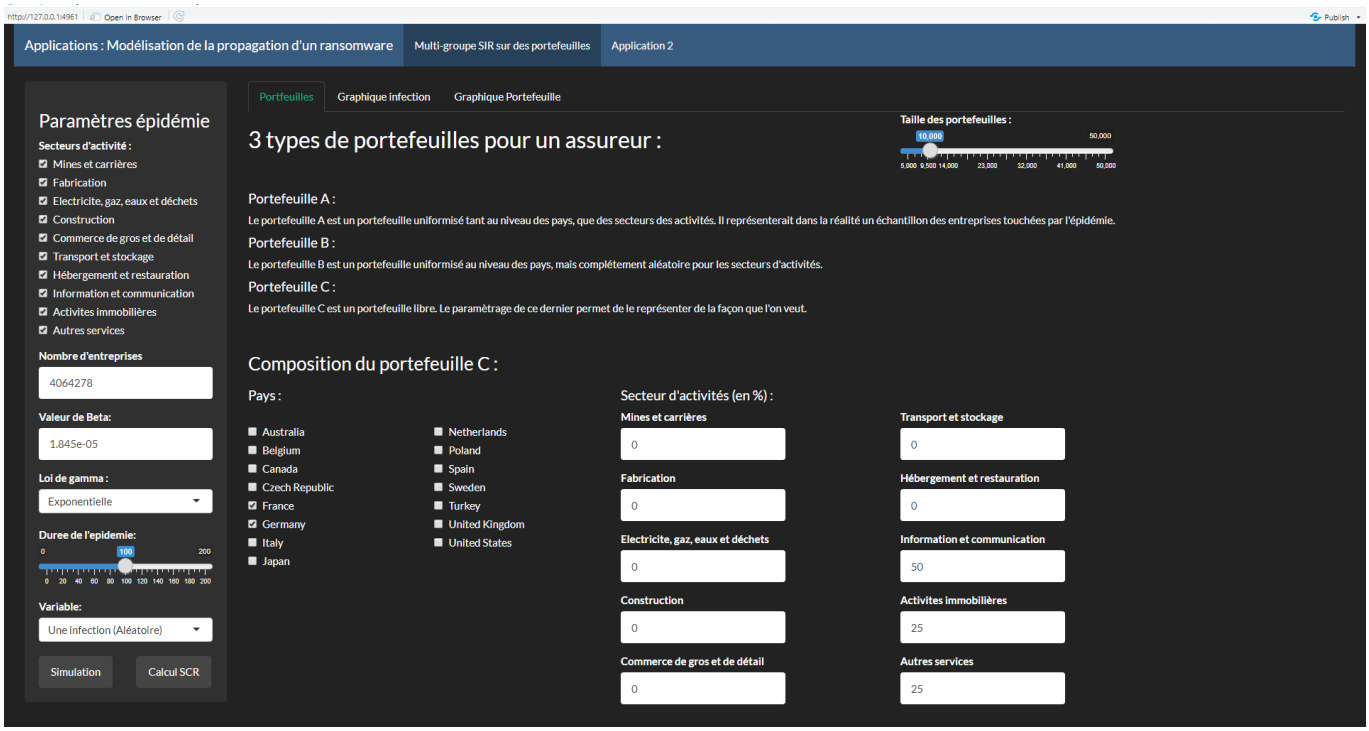

FIGURE 5.5 – L'application Rshiny permettant de tester différents paramètres pour la propagation d'un rançongiciel à travers trois portefeuilles.

La première sélection concerne les secteurs d'activités désirés. Il est nécessaire d'en cocher au moins 2. Dans les simulations du mémoire, tous les secteurs d'activités sont utilisés. Les prochains paramètres modifiables sont le β et la loi associée au γ. Ils varieront lors des simulations effectuées. Il est également possible de choisir la façon dont l'épidémie commence. Les différents choix sont expliqués dans la sous-section suivante.

Les 4 onglets présents ("Portefeuilles", "Graphique infection" , "Graphique Portefeuille" et "SCR") permettent de naviguer à travers cette application :

— **Portefeuilles :** Cet onglet décrit la composition des 3 portefeuilles imaginés et permet de composer le portefeuille C de la manière souhaitée,

— **Graphique infection :** Cet onglet affiche deux graphiques. Le premier illustre la courbe du nombre d'entreprises infectées à l'instant pour chaque secteur d'activités. Le second montre la courbe du nombre d'entreprises infectées à l'instant t,

— **Graphique portefeuille :** Cet onglet est composé de 4 graphiques. Les 3 premiers détaillent le nombre d'entreprises infectées pour chaque secteur d'activités pour chaque portefeuille. Le dernier est un histogramme rappelant le coût moyen d'une entreprise dans un portefeuille, le coût total ainsi que le nombre d'entreprises touchées par portefeuille,

— **SCR :** Cet onglet affiche deux graphiques. Le premier illustre la courbe du nombre d'entreprises infectées à l'instant pour chaque secteur d'activités. Le second montre la courbe du nombre d'entreprises infectées à l'instant t,

5.2.2 Début de l'épidémie

Comme déjà mentionné au cours du mémoire, le début de l'épidémie n'est pas forcément constaté à la première infection. Ainsi, un des paramètres de l'application permet de construire le début de l'épidémie. Le choix du premier infecté peut avoir des répercussions sur l'épidémie. Si un secteur d'activités est très propice à favoriser une épidémie infectant majoritairement les entreprises de son secteur d'activités, (i.e. la valeur de *proximité* vers lui-même est important), l'impact de la propagation du rançongiciel ne sera pas le même que si le premier infecté est issu d'un autre secteur d'activités. De plus, si le rançongiciel est dit *silencieux*, il est probable qu'au début de la propagation, plusieurs machines soient déjà infectées. Ainsi, l'application propose le choix entre 4 scénarios différents, prenant en compte les concepts expliqués ci-dessus :

— *une infection (aléatoire)* : Ce choix entraîne la sélection du secteur d'activités contenant le premier infecté par une loi uniforme discrète. Autrement dit, chaque secteur d'activités a une probabilité identique d'avoir une de ses entreprises comme patient zéro,

— *une infection (représentative)* : La probabilité que le patient zéro soit issu d'un secteur d'activités précis est proportionnelle au nombre d'entreprises présentes dans le secteur d'activités en question. Ainsi, plus le secteur d'entreprises comporte un nombre important de sociétés, plus la probabilité que le premier infecté appartienne à ce secteur est forte,

— *lot d'embrasement (aléatoire)* : De manière similaire au premier choix, la probabilité qu'un individu soit infecté au départ est équiprobable. Cependant, dans le cadre d'un rançongiciel *silencieux*, il y a plusieurs patients zéro. Ainsi, le processus d'infection est répété jusqu'à obtenir 0,05% d'entreprises infectées.

— *lot d'embrasement (représentative)* : De manière similaire au second choix, la probabilité qu'un individu soit infecté au départ est proportionnelle au nombre d'entreprises de son secteur d'activités. Cependant, dans le cadre d'un rançongiciel *silencieux*, il y a plusieurs patients zéro. Ainsi, le processus d'infection est répété jusqu'à obtenir 0,05% d'entreprises infectées.

Ces 4 options ajoutent une dimension supplémentaire aux différentes simulations. La différence entre un patient zéro ou des patients zéro au début de l'épidémie, ainsi que la provenance de leur secteur d'activités sont des facteurs ayant un fort impact sur le déroulé des simulations

5.2.3 Création de 3 portefeuilles différents

Lors des simulations effectuées, trois portefeuilles différents ont été utilisés. Les différences de composition des portefeuilles se basent sur la provenance des assurés tant au niveau des pays que des secteurs d'activités. La taille des 3 portefeuilles est identique et supposée à $N = 10000$. Cependant, elle peut être modifiée et peut varier de 5000 à 50000 assurés. La variété de provenances des assurés au sein des deux premiers portefeuilles est déjà fixée dans l'application, tandis que la construction du dernier portefeuille demeure totalement libre.

— *portefeuille A* : le portefeuille A représente un portefeuille de type *uniforme*. Il s'agit d'une sous-sélection de la population globale qui aurait exactement les mêmes proportions (tant au niveau des pays, que des secteurs d'activités). Ce portefeuille est une sous-représentation de la population globale.

— *portefeuille B* : ce portefeuille est une sous-représentation de la population globale en ce qui concerne les pays. Néanmoins, sa composition vis-à-vis des secteurs d'activités ne l'est pas. Chaque secteur d'activités est représenté dans les mêmes proportions. Ainsi, ce portefeuille a pour volonté de diversifier son risque au niveau des secteurs d'activités de façon uniforme,

— *portefeuille C* : dans les simulations, ce portefeuille sera uniquement composé d'entreprises françaises, dont la moitié sont dans l'information et communication, 25% dans des activités immobilières et 25% dans le commerce de gros et de détail.

	Mines et carrières	Fabrication	Électricité, gaz, eaux et déchets	Construction	Commerce de gros et de détail	Transport et stockage	Hébergement et restauration	Information et communication	Activités immobilières	Autres services
Portefeuille A (Uniforme au niveau des pays)	0,20%	9,18%	0,65%	14,57%	26,78%	6,21%	8,72%	4,42%	5,73%	23,55%
Portefeuille B (Uniforme au niveau des pays)	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%	10,00%
Portefeuille C (Uniquement français)	0,00%	0,00%	0,00%	0,00%	25,00%	0,00%	0,00%	50,00%	25,00%	0,00%

FIGURE 5.6 – Composition des 3 portefeuilles présents dans les simulations effectuées.

Le fait de proposer trois portefeuilles dont les stratégies de diversification des assurés sont totalement différentes a pour objectif d'exposer à quel point cela peut impacter la somme des montants des sinistres sur plusieurs scénarios. Il faut comprendre que l'intégration d'un assuré dans deux portefeuilles différents n'aura peut-être pas le même impact si l'épidémie ne touche pas toutes les entreprises.

5.2.4 Simulations

Pour rappel, la valeur du taux de guérison γ est dynamique comme expliqué dans la sous-section *Estimation du taux de guérison* γ et la valeur du taux de transmission β est fixée à $2,3 \times 10^{-5}$. Ce taux correspond à une approximation du scénario de type *WannaCry*. Il n'est pas le même que celui retenu, car comme déjà expliqué, il est appliqué à la matrice B dans le cadre d'un modèle SIR multi-groupes. Le nombre d'entreprises global ne change pas et vaut toujours 4 064 278. Les autres paramètres (loi de γ, durée de l'épidémie, le choix de l'infection au début de la propagation et la composition du portefeuille C) sont précisés au cours des différents scénarios.

5.2.4.1 Exemple d'une simulation

Les paramètres de cette première simulation sont les suivants :

— la loi du taux de γ est une loi exponentielle bornée. Lors des tirages, la moyenne de ce taux pour les 10 secteurs d'activités est de 0,92,
— la durée de l'épidémie est supposée à 60 jours,
— la première infection est unique (un seul patient zéro) et aléatoire,
— le portefeuille C est un portefeuille français composé de 50% d'entreprises issues de l'information et communication, 25% dans des activités immobilières et 25% dans le commerce de gros et de détail.

La simulation étudiée a touché en premier lieu une entreprise spécialisée dans *les autres services*. La figure suivante détaille comment la totalité des entreprises dans le monde ont été touchées et comment la différence entre les secteurs d'activités se traduit.

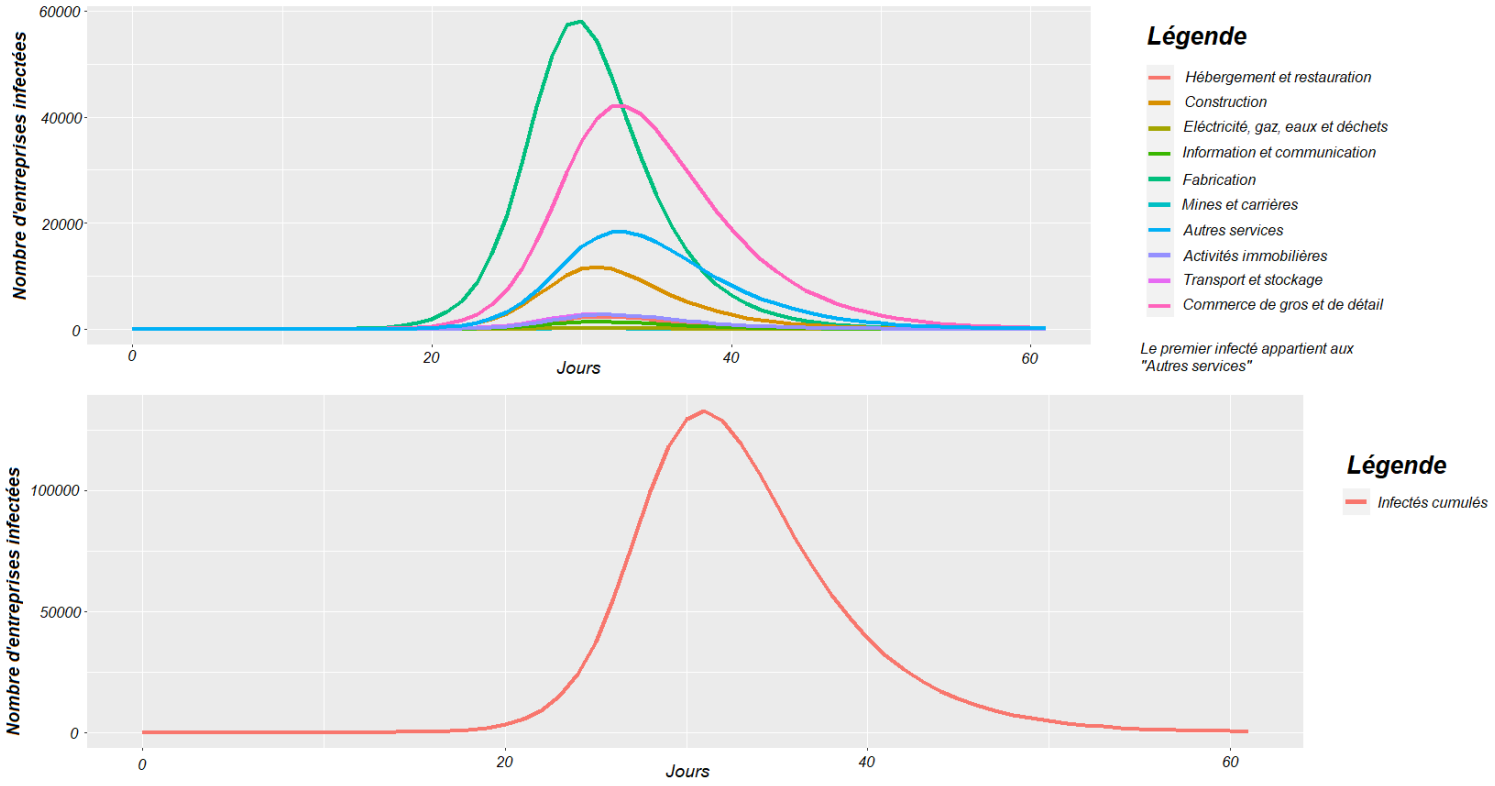

FIGURE 5.7 – Simulation 1 : nombre d'entreprises infectées selon les secteurs d'activités, et selon la population globale.

Le nombre d'entreprises infectées total est de 1007098, ce qui représente quasiment 24,78% de la population globale. Le secteur d'activités de la fabrication est beaucoup plus touché par le rançongiciel. Cela peut s'expliquer sa taille (ce secteur équivaut à 9% des sociétés potentiellement exposées au risque). Les secteurs d'activités les moins touchés dans cette simulation demeurent les sociétés appartenant à l'électricité, gaz, eaux et déchets et aux mines et carrières. Néanmoins, elles représentent respectivement seulement 0,6% et 0,19% des entreprises).

En reprenant la matrice B, il est observable que les secteurs les plus infectés n'ont pas une forte "proximité" avec les secteurs d'activités les moins touchés. La "proximité" évaluée entre les deux secteurs les plus touchés est de moins de 1%. Ainsi, une faible proximité avec le secteur d'activités le plus touché n'évite pas d'être épargnée par l'épidémie.

La figure suivante permet quant à elle de mieux comprendre la façon dont l'épidémie a touché les trois portefeuilles :

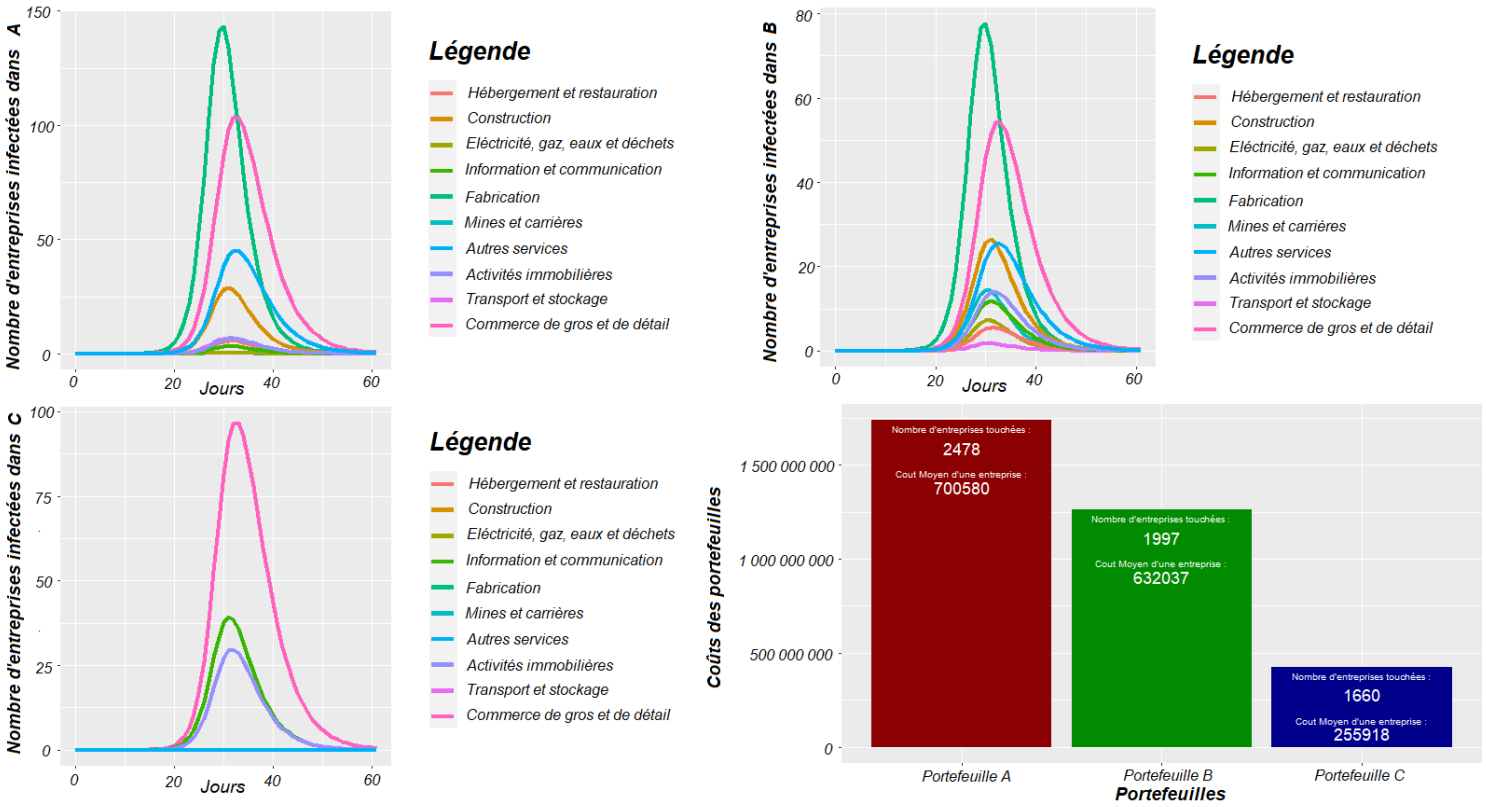

FIGURE 5.8 – Simulation 1 : Résultat de la propagation à travers les trois portefeuilles

Comme attendu, le secteur de la fabrication domine complètement les portefeuilles. Le portefeuille A, qui pour rappel a les mêmes proportions que la population globale en termes de diversité de pays et de secteurs d'activités, a un graphique similaire au précédent. Le portefeuille B, qui est uniformisé au niveau de ses secteurs d'activités, est finalement proche du graphique du portefeuille A. Seuls les secteurs d'activités les moins touchés ont une évolution différente comparée au portefeuille A. Enfin, pour le portefeuille C, le secteur de commerce de gros et détail est le plus touché même s'il ne représente que 25% des assurés.

En termes de coût financier (i.e. $\mathrm{N}_t = C \lim_{t \to +\infty} \mathrm{N}_t$) et de nombre d'entreprises infectées, le portefeuille A est le plus touché et le plus cher. Il s'approche des 24,78% d'entreprises touchées et la somme des sinistres est très élevée. Le portefeuille B est un peu moins touché par le rançongiciel que le portefeuille A. Logiquement, le coût financier est moins important, car le nombre d'entreprises sinistrées l'est aussi. Enfin, la diversification du portefeuille C lui permet d'être plus épargné. En effet, il n'est touché qu'à 16,6% et son coût est bien moins élevé. Cela s'explique par un nombre d'entreprises touchées plus faible, mais également par le fait que les sinistres de rançongiciel en France coûtent en moyenne 30% moins cher. Enfin, les secteurs d'activités présents dans le portefeuille C ont en moyenne des sinistres moins onéreux.

Toutefois, il est également possible d'estimer le coût mesurant la capacité maximum de l'assureur à assister ses assurés. Ce coût consiste à ce qu'à partir d'un certain seuil, l'assureur n'est plus capable de garantir une aide à tous ses assurés. En supposant que cette limite soit de 110 pour chaque portefeuille, si le nombre d'entreprises infectées en même temps dépasse ce seuil, alors les coûts supplémentaires sont beaucoup plus importants.

Si $K = 200$ et J_t correspond au nombre d'assurés infectés à l'instant t, alors le coût de saturation

(comme défini lors du chapitre 3) est le suivant :

$$C_2 = \mathbb{1}_{\sup t} J_t \geqslant K$$

— pour le portefeuille A : le nombre d'entreprises infectées et non assistées est estimé à 811,
— pour le portefeuille B : le nombre d'entreprises infectées et non assistées est estimé à 533,
— pour le portefeuille C : le nombre d'entreprises infectées et non assistées est estimé à 0.

En supposant que chaque entreprise infectée non assistée par l'assureur entraîne une perte supplémentaire de 0,5 fois le coût financier (C_1), alors les coûts finaux sont les suivants :

Portefeuille	C_1	C_2	**Total**
A	1 736,7 M	284,19 M	2 020,90 M
B	1 262,17 M	168,43 M	1 430,61 M
C	424,82 M	0,00 M	424,82 M

5.2.5 Exemple de différentes simulations

Certaines réalisations contiennent des résultats totalement différents. L'épidémie peut s'arrêter très rapidement et presque ne pas se propager, tout comme elle peut toucher quasiment l'entièreté de la population. On s'intéresse ici à des simulations dites extrêmes.

La figure suivante illustre le fait que dans certains cas l'épidémie s'arrête rapidement. En effet, lorsque les paramètres du modèle ne favorisent pas la propagation de l'épidémie, alors cette dernière décroît directement et n'affecte quasiment pas les entreprises.

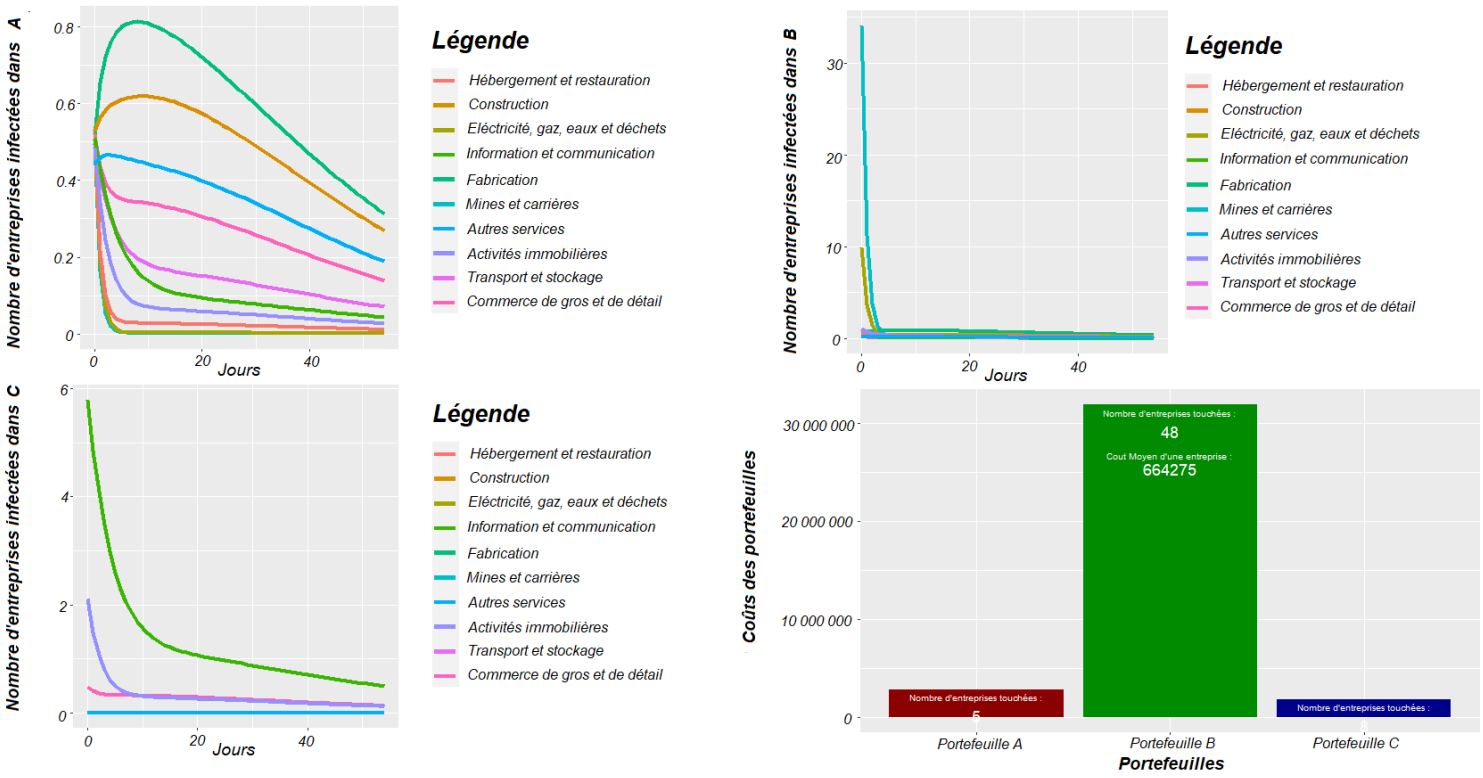

FIGURE 5.9 – Résultat d'une simulation où l'épidémie décroît rapidement.

La figure suivante illustre le fait que dans certains cas l'épidémie dure dans le temps. En effet, lorsque les paramètres du modèle favorisent la propagation de l'épidémie, alors l'épidémie peut s'éterniser sans pour autant être virulente.

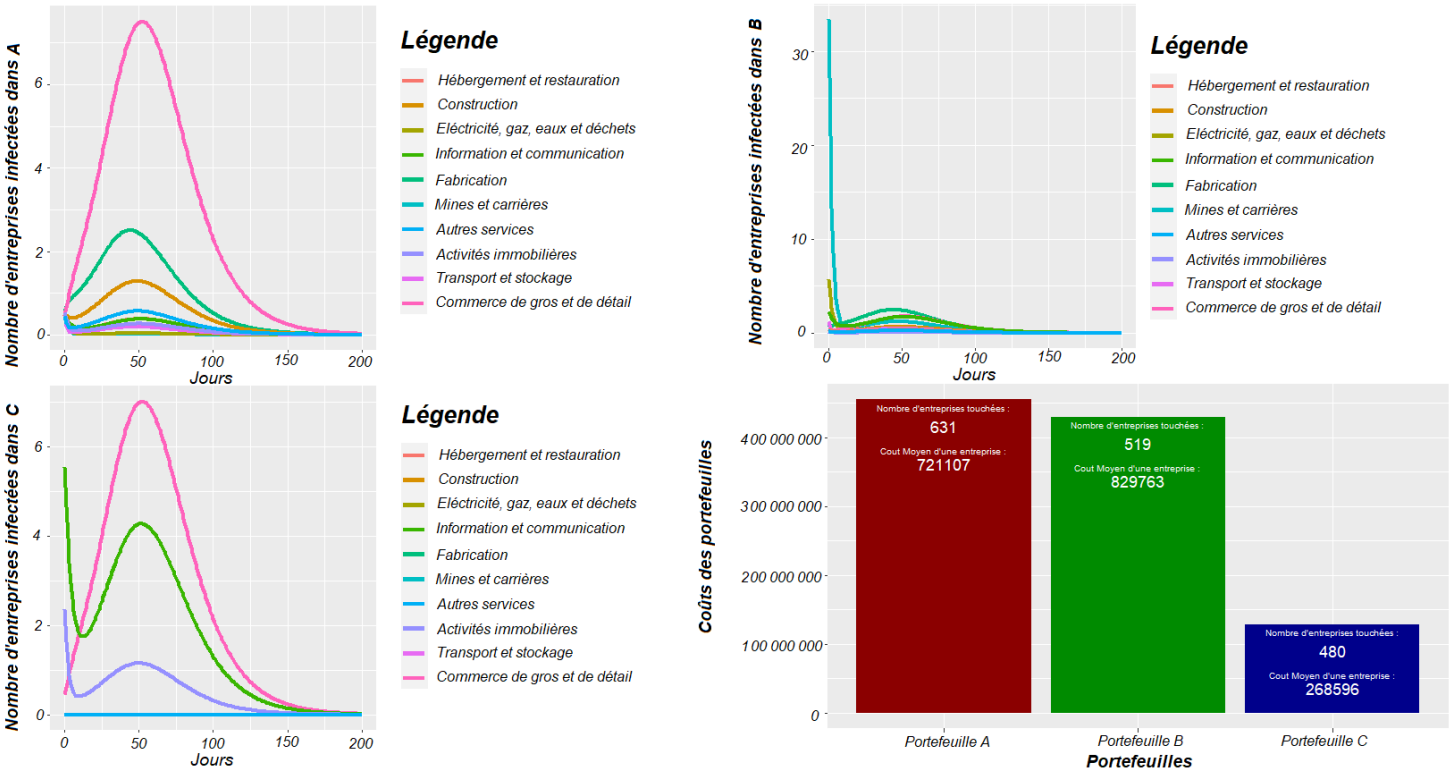

FIGURE 5.10 – Résultat d'une simulation où l'épidémie décroît lentement sans être virulente.

Les deux figures précédentes mettent donc en avant les simulations les plus extrêmes. La première différence entre ces deux scénarios est la durée de l'épidémie. La première est basée sur une soixantaine de jours, tandis que celle qui suit dure presque 200 jours. De plus, le nombre d'assurés infectés dans les portefeuilles est entre 75% et 80% moins important pour l'épidémie de 60 jours.

Le deuxième cas peut sembler contre intuitif, car l'épidémie est lente, mais ne touche pas beaucoup d'entreprises. Cela s'explique par la valeur du taux de transmission γ. S'il est faible, alors les entreprises sont contagieuses pendant un laps de temps élevé. Ce phénomène devrait favoriser la propagation du rançongiciel. Cependant, quand le taux de transmission est trop faible, alors l'épidémie ne peut pas se propager. Ce style de scénario permet de justifier la pertinence du coût C_2.

5.2.6 Résultat des simulations

50 000 simulations ont été réalisées à travers l'application *Rshiny*. Afin de gagner en temps de calcul, la parallélisation a été utilisée. Cette optimisation est détaillée dans l'annexe B.

Les paramètres énoncés précédemment peuvent évoluer au cours des 50 000 simulations. Plus précisément, le choix de ces paramètres est aléatoire et équiprobable. Afin de comparer tous ces paramètres, 50 000 simulations ont été réalisées afin de pouvoir distinguer l'effet des impacts qu'ils peuvent avoir. Les impacts sont purement financiers et correspondent au coût C_1.

Pour rappel, les SCR estimés dans ce chapitre équivaut au quantile à 99,5%, autrement dit ils

correspondent à la 49750$^{\text{ème}}$ simulation lorsque ces dernières sont ordonnées de façon croissante vis-à-vis des montants totaux des sinistres.

	Portefeuille A	Portefeuille B	Portefeuille C
Min	0,00 €	0,00 €	0,00 €
Moyenne	1 061,52 €	1 187,39 €	297,12 €
Mediane	1 086,19 €	1 012,82 €	287,50 €
Ecart-type	642,68 €	893,73 €	200,34 €
SCR	1 987,01 €	3 691,04 €	795,05 €
Max	2 160,83 €	5 953,35 €	832,88 €

FIGURE 5.11 – Simulations : Détails des différentes informations en termes de coût totale des sinistres sur les 50 000 simulations réalisées. Le coût est exprimé en millions.

Sur ces 50 000 simulations, certaines proposent des résultats où l'épidémie s'arrête rapidement comme expliqué précédemment. Quelques entreprises sont infectées, mais la contamination stoppe brutalement et n'infecte pas les portefeuilles imaginés. Ce phénomène explique que le minimum soit de 0 euro.

La première observation est que le portefeuille C, uniquement français et composé de 3 secteurs d'activités, est largement moins onéreux que les autres ; il est même 25% moins coûteux. Cette différence s'explique par un coût moyen moins élevé, mais également par une propagation au sein du portefeuille C moins importante. Le choix des pays et du secteur d'activités est donc un choix primordial dans la constitution du portefeuille, ainsi que dans la tarification à proposer.

La ressemblance entre les montants des portefeuilles A et B est finalement logique. L'écart-type démontre bien que la composition du portefeuille B propose des simulations avec des montants totaux plus différents. Outre le nombre d'assurés touchés dans ces portefeuilles, la composition joue un rôle majeur. S'il n'y a pas de sélection lors de la souscription, la valeur du SCR peut grandement varier. Comme constatée, la moyenne est quasiment identique, tandis que le SCR demandé par le portefeuille B est quasiment le double que celui du portefeuille A.

Afin de comparer les impacts que peuvent avoir les paramètres de l'application (lois des taux de guérison et choix du début de l'épidémie), 50 000 simulations ont été réalisées pour chaque paramètre qu'offre le modèle. Autrement dit, il est possible de comparer les valeurs de la figure précédente selon chaque paramètre.

	Min	Moyenne	Mediane	Ecart-type	SCR	Max
Exponentielle	0,00 €	1 144,83 €	1 189,76 €	571,83 €	2 327,48 €	3 032,72 €
Weibull	0,00 €	752,20 €	683,63 €	542,49 €	2 076,01 €	2 586,82 €
Log Normal	0,00 €	760,69 €	695,90 €	553,96 €	2 095,15 €	3 379,95 €
1 infection (aléatoire)	0,00 €	849,27 €	799,52 €	579,72 €	2 208,75 €	2 989,44 €
1 infection (représentative)	0,00 €	850,67 €	799,73 €	578,84 €	2 212,54 €	2 657,67 €
Lot d'embrassemnt (aleatoire)	1,98 €	853,89 €	800,20 €	579,85 €	2 222,84 €	2 903,31 €
Lot d'embrassemnt (représentatif)	1,36 €	848,70 €	798,25 €	579,26 €	2 208,27 €	2 898,31 €

FIGURE 5.12 – Simulations : Détails des coûts selon les 50 000 simulations réalisées pour chaque paramètre et chaque portefeuille. Le coût est exprimé en millions.

Le choix du début de l'épidémie influe sur le coût minimum des 50 000 simulations. En effet, le fait que l'épidémie n'ait pas lieu, n'empêche pas l'assureur d'avoir plusieurs sinistres. Cependant, une épidémie silencieuse à ses débuts n'a pas réellement d'impact sur le reste des indicateurs en termes de coût La différence entre aléatoire et représentative n'est pas vraiment visible et ne semble pas justifier un changement de la propagation au sein des 3 portefeuilles.

Enfin, pour ce qui est des lois, il existe une réelle différence entre l'exponentielle et les deux autres. En effet, le coût est plus important du côté de la loi exponentielle. Cela peut s'expliquer par le fait que la réaction est plus lente et que les entreprises sont moins rapides à réagir. C'était justement le résultat attendu. Du côté, de la loi de Weibull et de la log-normale, les résultats sont très proches. Même si la log-normale est censée être plus virulente en termes de coût que la Weibull, la similarité peut s'expliquer par deux options. Une mauvaise calibration des paramètres ne permettant pas de mettre en évidence le comportement des assurés, ou alors qu'à partir d'un certain moment, un comportement plus prudent de la part de l'assuré n'a plus un impact aussi fort que précédemment.

5.3 Transfert du risque à travers un traité non-proportionnel

5.3.1 Structure du traité et rappels succincts

À la vue de l'impact que peut avoir ce type de scénario, un assureur peut choisir de transférer une partie de ce risque vers un réassureur. C'est dans cette démarche que ce mémoire propose une application liée à la réassurance.

Le traité imaginé sera un traité non-proportionnel de type Excédent de Sinistre, appelé également traité *XS*. L'objectif de cet exercice est d'observer l'impact d'un traité XS sur des portefeuilles où les secteurs d'activités et les provenances des pays sont différents.

Bien conscient que les coûts estimés sont éloignés de la réalité, les différents niveaux de primes commerciales selon les caractéristiques du portefeuille restent un bon indicateur. Les paramètres du traité sont fictifs. Les composantes du traité sont les suivantes :

Paramètres	**Valeur**
Priorité	50,00 M
Portée	500,00 M
Nombre de reconstitutions	1
Prime de la reconstitution	5,00M
Coefficient de chargement pour risque (k)	10%
Frais de chargement (θ)	20%

En supposant que X soit le coût de l'évènement, le montant à la charge du réassureur dans un traité XS est défini tel que :

$$\begin{cases} 0 & si\ X \leqslant\ priorité \\ X - priorité & si\ priorité\ \leqslant X \leqslant portée + priorité \\ portée & X \geqslant portée + priorité \end{cases}$$

D'une manière plus simple, il est possible d'affirmer que le montant à la charge du réassureur est :

$$\min[\max(X - priorité\ , 0), portée]$$

Pour rappel, lorsque la portée est consommée par un évènement, la cédante n'est en principe plus protégée si un autre évènement de plus survient la même année. Toutefois, chaque nombre de reconstitutions permet à la cédante de renouveler la couverture en s'acquittant de la prime de reconstitution.

Dans cette application, il est supposé que ce traité est un *XS* par évènement. Il n'y a pas de clause de limitation géographique et la clause de limitation temporelle est supérieure à la durée de l'épidémie.

Le principe de l'exercice repose sur le fait d'estimer :
— la charge brute représentant les engagements de la cédante vis-à-vis des assurés,
— la charge cédée correspondant au montant pris en charge par le réassureur,
— la charge nette qui est la différence de la charge brute et de la charge cédée.
Enfin, il est possible d'estimer la prime commerciale en évaluant l'écart-type de la charge cédée. Pour rappel, la prime commerciale s'évalue de la façon suivante :

$$Prime\ commerciale\ = \frac{Prime\ Pure + k * \sigma_{charge\ cédée}}{1 - \theta}$$

où $\sigma_{charge\ cédée}$ est l'écart-type de la charge cédée simulée.

5.3.2 Modélisation coût x fréquence d'un évènement

Cette sous-section permet la modélisation en plusieurs étapes de la tarification de la couverture non-proportionnelle par le biais d'une approche par simulation. Ces étapes sont divisées en 3 parties.

5.3.2.1 *Event Loss Table* (ELT)

La première étape consiste à créer une table *Event Loss Table* (ELT). Il s'agit d'une table contenant les pertes causées par chaque évènement. Plus précisément, l'ELT livre des informations comme le coût moyen, la volatilité des pertes, ou encore le montant maximal assuré.

La table de l'ELT est obtenue en reprenant les 50 000 simulations de la section précédente. Les résultats sont accessibles en consultant la figure 5.11 rappelant les différents indicateurs statistiques pour chaque portefeuille.

5.3.2.2 Modélisation de la fréquence

La seconde phase a pour objectif de simuler la fréquence annuelle. Pour un grand nombre d'années, la quantité d'évènements est probabilisée par une loi de fréquence. Pour les évènements associés aux catastrophes *man-made*, l'hypothèse d'une fréquence de la loi de Poisson est raisonnable.

Les données Cyber concernant les rançongiciels sont trop pauvres pour permettre l'estimation du paramètre λ de la loi de Poisson. Cependant, lors des 20 dernières années, 3 rançongiciels auto-répliquant de grande ampleur ont été signalés. Aussi, λ sera estimé à $0,15$ correspondant à 0,15 évènement par an.

5.3.2.3 *Year-Event Loss Table* (YELT)

La dernière étape est l'obtention de la table *Year-Event Loss Table* (YELT). Elle résulte de la table ELT et de la modélisation de la fréquence. Pour chaque année simulée, un nombre d'évènements lui est associée d'après la loi de Poisson. Chaque évènement correspond à une simulation de pertes provenant de la table ELT. Si l'année simulée contient plusieurs évènements, alors la charge totale équivaut à la somme des pertes des différents évènements. Autrement dit, pour établir la table YELT, il suffit donc d'agréger annuellement les charges individuelles des évènements.

5.3.3 Résultats du traité XS sur le portefeuille A et C

Après avoir appliqué le traité XS aux différents évènements du portefeuille A et C via la table YELT générée, il est possible de visualiser la distribution des charges cédées, brutes et nettes. Les figures suivantes ont été obtenues en triant les valeurs des charges cédées par ordre croissant. Pour favoriser la lecture des figures, les valeurs des charges cédées sont triées selon les valeurs des charges brutes, lorsqu'elles sont identiques. Les pics observables sur les figures sont résultent du fait que la charge cédée n'est pas une fonction croissante de la charge brute.

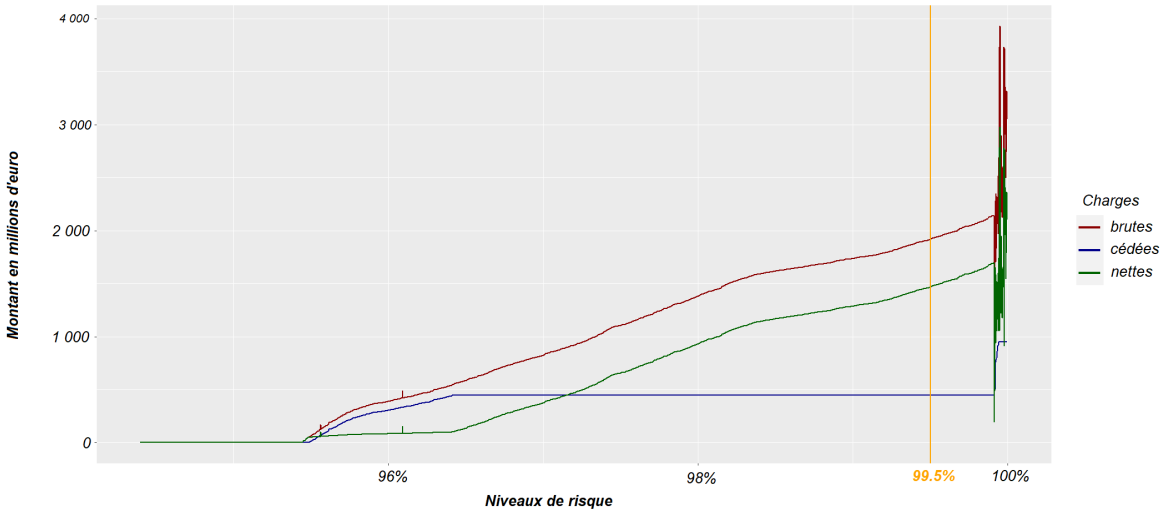

FIGURE 5.13 – Distribution des différentes charges du traité XS pour le portefeuille A

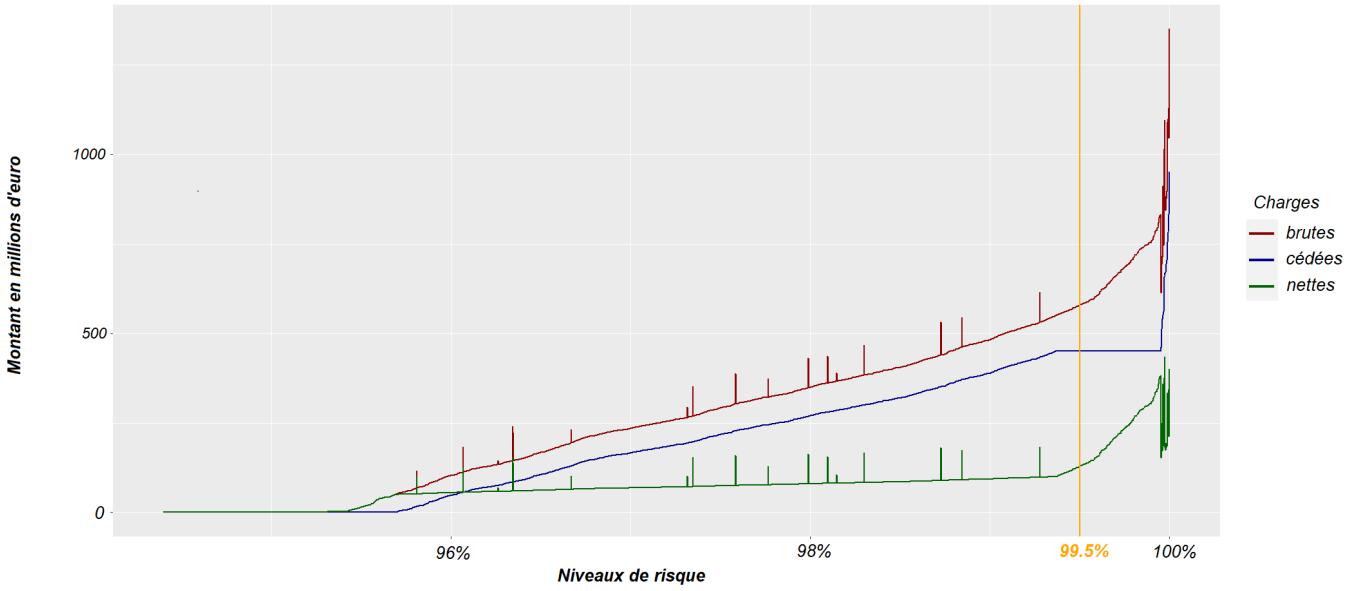

FIGURE 5.14 – Distribution des différentes charges du traité XS pour le portefeuille C

Pour les deux portefeuilles, seulement 4,5% des simulations donnent lieu à une charge cédée non nulle. Les couches sont alors peu travaillantes. La grande différence entre les deux portefeuilles est la reconstitution de la couverture. Pour le portefeuille A, elle se déclenche pour les 3,6% dernières simulations, tandis que seulement 0,01% des simulations donnent lieu à la reconstitution pour le portefeuille C.

Indicateurs	**Portefeuille A**	**Portefeuille C**
Quantile 99,5% (charge brute)	1 910,06 M	579,18 M
Quantile 99,5% (charge nette)	1 453,61 M	133,25 M
Quantile 99,5% (charge cédée)	450,00 M	450,00 M
Ecart-type de la charge cédée	90,50 M	60,11 M
Prime pure	18,98 M	11,05 M
Prime commerciale	35,04 M	21,33 M

La charge cédée n'étant pas une fonction croissante des autres charges, la différence entre le quantile de la charge brute et de la charge cédée n'est pas égale au quantile de la charge nette.

Pour des primes commerciales s'élevant respectivement à 35,04 et 21,33 millions pour les portefeuilles A et C, le gain économique (correspondant à la différence entre le quantile 99,5% de la charge brute et de la quantile 99,5% de la charge cédée) est proche de 450 millions. Cette couverture de risque opérationnel de rançongiciel est donc intéressante pour des assureurs.

L'application permet de mettre en évidence la différence des primes entre les deux portefeuilles selon leur composition. Le portefeuille C est exclusivement français et restreint à des secteurs d'activités précis (seulement 3). C'est ce choix qui permet à ce portefeuille de réduire ses charges brutes lors des niveaux de risque les plus élevés. Ce phénomène explique en partie pourquoi la prime du portefeuille A est plus élevée, bien que le traité de réassurance se déclenche au même niveau de risque pour les deux portefeuilles.

Conclusion

Le risque de rançongiciel est le risque émergent de demain pour les assureurs. De nombreux experts s'attendent à ce que les prochaines catastrophes économiques soient provoquées par des attaques Cyber massives. Les statistiques et bases de données étudiées dans ce mémoire justifient la difficulté pour un assureur à appréhender et maîtriser ce nouveau risque. C'est dans cette dynamique que s'inscrit le mémoire, dont la finalité est de proposer une modélisation innovante de la propagation d'un rançongiciel s'auto-diffusant.

Dans un premier temps, l'objectif a été de définir un type de modèle mathématique répondant au plus prés aux caractéristiques des risques de rançongiciel. Le modèle épidémiologique SIR à un groupe répondait au mieux à ces exigences mais nécessitait d'être généralisé à plusieurs groupes. Ce sont ces éléments qui ont servi à développer une approche actuarielle. Cette dernière permet de mettre en exergue les coûts financiers, le risque de saturation et l'influence du comportement de l'assuré sur la propagation. En théorie, l'assureur pourrait minimiser la diffusion du rançongiciel en ciblant des assurés "supraconducteurs" par l'analyse des spectres laplaciens.

Une remarque récurrente au sein de ce mémoire est que le risque de rançongiciel souffre du manque de données. Un retraitement approfondi des bases de données *PRC* et *VERIS* n'a pas permis d'obtenir de résultats probants. Néanmoins, l'utilisation des ressources comme les statistiques *Sophos*, les données de l'*OCDE* et l'historique des transactions *Bitcoin* ont permis la calibration des paramètres du modèle SIR et l'élaboration d'applications actuarielles. La première traite des simulations de la propagation d'un rançongiciel au sein de trois portefeuilles d'assurés fictifs. La seconde porte sur le transfert de ce risque à travers un traité non-proportionnel.

La détermination des assureurs à proposer des produits d'assurances adaptés au risque Cyber s'accroît. De plus, les TPE et PME qui représentent un marché non-négligeable n'ont pas la culture de ce risque. Fort de ce constat, certains Cyber-insurtech soulignent l'importance de coupler une formation et un diagnostic informatiques à l'assurance Cyber. C'est ainsi qu'ils réussissent à démocratiser les contrats d'assurance Cyber auprès des TPE et PME

Enfin il appartient peut-être aux institutions nationales et internationales de prendre des mesures permettant de constituer des bases de données Cyber publiques et également de dresser un inventaire de la situation de la Cyber-assurance en vue de la structurer, comme le soulignait, en 2021, l'ex-députée Valérie Faure-Muntian.

Bibliographie

[1] G. Arcas, *Rançongiciels 101*, 2020.

[2] T. Bastard, *Modélisation du risque cyber de perte de données à caractère personnel, modèle de tarification, inclusion dans le bgs et proposition de scénarios de stress pour l'orsa*, 2021.

[3] C. Bayette and M. Monticelli, *Modélisation d'une épidémie (partie 1 et partie 2)*, 2020.

[4] Y. Bessy-Roland, *Modélisation stochastique individuelle de sinistres cyber*, 2019.

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

[6] T. Cohignhac and N. Kazi-Tani, *Laplacian spectra of graphs and cyber-insurance protection*, 2020.

[7] M. A. Fahrenwaldt, S. Weber, and K. Weske, *Pricing of cyber insurance contracts in a network model*, 2018.

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

[9] C. Hillairet, O. Lopez, L. d'Oultremont, and B. Spoorenberg, *Cyber contagion : impact of the network structure on the losses of an insurance portfolio*, 2020.

[10] G.-G. Kolaye, C. Mbuge, J.-C. Kamgang, and S. Bowong, *Modélisation et simulation multi-agent de la propagation d'une épidémie de choléra : cas de la ville de ngaoundété*, 2020.

[11] B. Longet, *Les enjeux de la qualité des données (acpr – direction des contrôles spécialisés et transversaux)*, 2016.

[12] P. Magal, O. Seydi, and G. Webb, *Final size of a multi-group sir epidemic model : Irreducible and non-irreducible modes of transmission*, 2018.

[13] P. V. Mieghem, J. Omic, and R. Kooji, *Virus spread in networks*, 2009.

[14] F. Planchet, *Assurance non vie, le modèle collectif*, 2003.

[15] Ponemon and IBM, *Globast cost of a data breach report*, 2019.

[16] F. Pons, *Etude actuarielle du cyber-risque*, 2014.

[17] H. Rabaï, R. Charrier, and C. Bertelle, *Etude de la propagation d'une perturbation dans un réseau d'interaction formé par un système multi-agent*, 2015.

[18] L. Rass and J. Radcliffe, *Spatial deterministic epidemics*, 2003.

[19] W. Sarakorn and I. Tang, *No one set of parameter values can simulate the epidemics due to sars ocurring at different localities*, 2008.

[20] Fédération française de l'Assurance, *Cartographie 2020 des risques émergents pour la profession de l'assurance et de la réassurance*, 2020.

[21] ITR manager, *Le nombre d'attaques ddos a augmenté de 128 % en france par rapport à 2019*, 2019.

[22] Le gouvernement français, *Prévention des risques majeures.*

[23] Privacy Rights Clearinghouse, *Website of prc.*

[24] Sophos, and Vanson Bourne, *État des ransomwares 2020*, 2020.

[25] VERIS (Vocabulary for Event Recording and Incident Sharing), *Website of veris.*

[26] H. Weiss, *The sir model and the foundations of public health*, 2013.

Table des figures

Annexe A

Exploration des bases PRC et VERIS

Cette annexe a été créée et écrite afin qu'un lecteur puisse effectuer un retraitement similaire. Chaque étape est détaillée et beaucoup d'informations sont présentes pour effectuer une exploration similaire. Bien sûr, le retraitement effectué dans ce mémoire est loin d'être parfait et une multitude de techniques peuvent être utilisées pour l'améliorer.

PRC

A.0.1 Rappel :

Comme présentée lors du chapitre 4, la base de données PRC *Privacy Rights Clearinghouse* a été téléchargée depuis leur site officiel (`https://privacyrights.org/data-breaches`). La version *csv* a été utilisée et est datée du 4 juin 2021. Elle comporte 9 015 sinistres, ainsi que 13 champs.

Le script R qui a permis de réaliser ce retraitement est disponible sur le *Github* suivant : `https://github.com/GeoffreyBard/RetraitementCyber`. Il se nomme *Prc.R*. Ce script est mis à disposition afin de pouvoir garder une sauvegarde du retraitement effectuée. De plus, la base de données (datant de juin 2021) est également mise à disposition sur le lien *Github*.

Puisque le retraitement est nettement détaillé dans le chapitre 4 pour la base PRC, il n'a pas été jugé nécessaire de détailler le code et la manière dont le retraitement a eu lieu. À noter qu'au début du script *Prc.R*, le code permettant d'obtenir le nuage de mot correspondant au champ lexical du rançongiciel est disponible et fonctionnelle.

VERIS

A.0.2 Rappel :

Comme présentée lors du chapitre 4, la base de données VCDB *The Veris Community Database* a été téléchargée depuis leur site officiel (`http://veriscommunity.net/`). La version *csv* a été utilisée et est datée du 26 juin 2021. Elle comporte 8 198 sinistres, ainsi que 2 441 champs.

Le script R qui a permis de réaliser ce retraitement est disponible sur le *Github* suivant : `https://github.com/GeoffreyBard/RetraitementCyber`. Il se nomme logiquement *Veris.R*. Les fonctions et la manière dont le retraitement a été fait sont loin d'être optimales. Ce script est mis à disposition afin de pouvoir garder une sauvegarde du retraitement effectuée. De plus, la base de données (datant de juin 2021) est également mise à disposition sur le lien *Github*.

A.0.3 Exploration et retraitement :

La première manipulation permettant de vérifier si le sinistre Cyber est bel et bien un évènement dû à un rançongiciel, a été de regarder si le champ noté *action.malware.variety.Ransomware* était vrai. Parmi les 8 198 sinistres, 147 répondent à ce critère. Ensuite, une liste de rançongiciels connus a été utilisée pour voir s'ils n'étaient pas présents dans la description de l'évènement. 15 sinistres sont le résultat d'un de ces rançongiciels. Cependant 13 d'entre eux étaient déjà parmi les 147 sinistres évoqués ci-dessus. Ainsi, ce filtre rapporte que 2 sinistres supplémentaires sont bien le fruit d'un rançongiciel. Le troisième retraitement s'effectue sur la présence du terme *ransom* dans le résumé du sinistre, i.e. le champ *summary*. 129 sinistres ont ce terme dans la description de leur évènement. Toutefois, 111 répondaient déjà aux deux critères précédents. Ainsi, le nombre de nouveaux sinistres causés par un rançongiciel trouvés s'établit à 18.

La base de données, suite à ces retraitements, se retrouve avec 167 évènements pour toujours 2 441 champs.

Une autre base de données (disponible sur le *Github* suivant `https://raw.githubusercontent.com/lukes/ISO-3166-Countries-with-Regional-Codes/master/all/all.csv`) contient tous les pays du monde, ainsi que leur abréviation en 2 et 3 lettres (i.e, alpha.2 et alpha.3). Ces abréviations s'appellent code ISO et sont internationales. Elles permettent de différencier les pays avec peu de caractère, ce qui peut être utile pour de nombreuses applications, comme les sites internet. La base VCDB possède 250 champs qui indiquent le lieu du sinistre. Comme expliqué dans l'exemple du chapitre 4, un champ permet d'indiquer si le sinistre a eu lieu dans ce pays ou non. Ces champs s'intitulent *victim.country."alpha.2"*. En utilisant, le code ISO de la base de données *Github* et à l'aide d'un petit script R astucieux, il est possible d'obtenir un nouveau champ à la base VCDB : la localisation du sinistre. Cette localisation est le nom exact du pays. En réalité, toutes ces étapes ont été nécessaires, afin d'avoir le nom anglophone des pays, permettant d'utiliser un package R *ggplot2* qui a permis de réaliser les figures où le nombre de sinistres par pays est indiqué à travers un planisphère.

À partir de ce nouveau champ, il a été créé un autre *data frame*. Seul le champ *pays* est présent. Comme son nom l'indique, il permet de connaître la localisation de l'évènement. La date du sinistre est récupérée à partir du champ de VCDB *timeline.incident.year*. D'autres variables ont été récupérées de la même manière que la date. Il s'agit du nombre de DCP (à partir de *attribute.confidentiality.datatotal*), du secteur d'activités (à partir de *victim.industry.name*) et du montant du sinistre (à partir de *impact.overall amount*).

Pour récupérer le nombre d'employé présent dans l'entreprise victime du rançongiciel, plusieurs champs de VERIS ont été utilisés. En effet, la base VCDB possède les champs s'intitulant *victim.employee count.x.to.y* où x et y sont deux nombres représentant l'intervalle du nombre d'employés de l'entreprise en question. La décomposition va de 1 à plus de 100 000, avec 8 intervalles possibles. Pour simplifier ce nombre de champs, une variable catégorielle a été imaginée. Elle est découpée en 5 niveaux qui sont les suivants :

— 1 - 100,
— 101 - 1 000,
— 1 001 - 10 000,
— 10 001 - 50 000,
— 50 000 - 100 000.

À partir de ces éléments, un nouveau champ compose le *data frame* créé.

Une autre variable ajoutée au *data frame* qualifie la sûreté des différentes informations sur le sinistre. Elle est construite à partir des champs *confidence.High*, *confidence.Medium*, *confidence.Low* et

confidence.None. Cette nouvelle variable étant catégorielle, elle prend la deuxième partie du nom du champ pour lequel l'information est vraie (Autrement dit, elle vaut soit "High", "Medium", "Low", ou NA).

Enfin, pour chaque sinistre ayant eu lieu dans le même pays, le nombre d'attaques est indiqué. Ainsi, il est possible de connaître le nombre de sinistres de rançongiciel présent dans la base VCDB dans un pays en particulier. Cette variable permet également de tracer plusieurs figures du chapitre 4.

Finalement, le script de retraitement de la base de VCDB permet de récupérer les sinistres causés par un rançongiciel et de garder un minimum d'information utile à un assureur. Pour rappel, la nouvelle base de données obtenue comporte 167 sinistres pour 8 champs qui sont la localisation, la date, le nombre de DCP en jeu, le secteur d'activités, la perte en dollar, le nombre d'employés, le niveau de confiance des informations précédentes et le nombre de sinistres dans le pays en question.

Annexe B

Application : *Rshiny* et fonctionnement

Cette annexe a été créée et écrite afin qu'un lecteur puisse manipuler l'application. Du lancement, au fonctionnement, un maximum d'informations a essayé d'être partagé au sein de cette annexe.

Utilisation (Github, Packages, Lancement)

Comme mentionné lors du chapitre 5, l'application est disponible en open source sur le *Github* suivant : `https://github.com/GeoffreyBard/Cyber-Ransomware-Model`. Il n'y a qu'une seule branche (*main*) et la dernière version est la plus aboutie.

B.0.1 Présentation des fichiers

L'ensemble des fichiers composant l'application contient plusieurs fichiers et dossiers. Des fichiers ne sont pas propres au fonctionnement du *Rshiny*, mais ont seulement un impact sur l'utilisation du *Github*. Plus précisément, la liste des fichiers et dossiers est la suivante :

— un dossier *DatabaseAvant* comprenant toutes les bases de données brutes, c'est à dire, avant retraitement,
— un dossier *DatabaseAprès* contenant toutes les bases de données retraitées,
— un dossier *www* permettant un affichage particulier sur l'application,
— 4 scripts R permettant de lancer l'application et de faire tourner la modélisation.

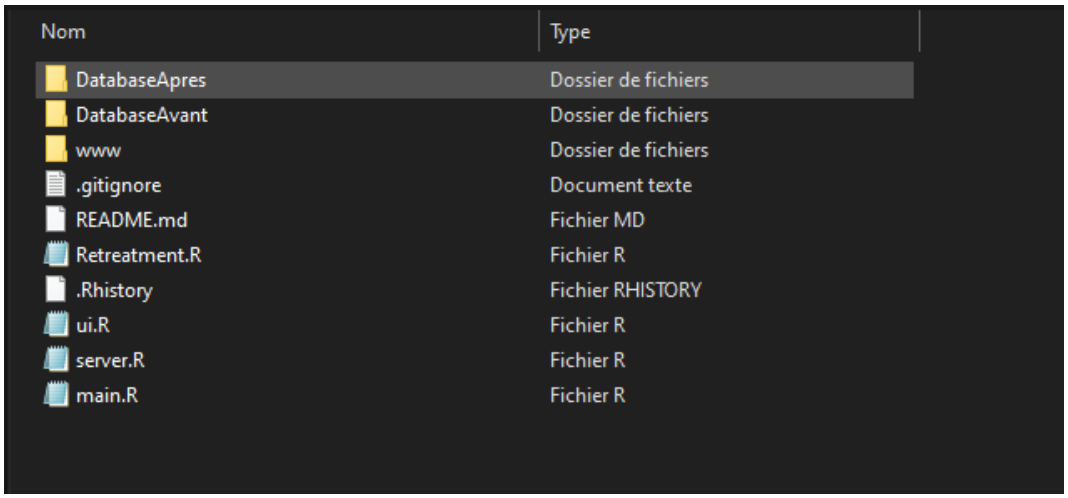

FIGURE B.1 – Liste des différents fichiers et dossiers composant l'application

Le dossier *DatabaseAvant* est composé de quatre fichiers de type *csv*. La première base de données se nommant *exrate.csv* contient l'ensemble des conversions des monnaies vers le Dollar américain. Les valeurs sont une moyenne lissée sur l'année 2015. Le second fichier *forex.csv* permet la création du fichier précédent. Il contient la même information, mais la valeur n'est pas unique, mais propre à chaque mois de 2001 à 2021. Un fichier *turnover.csv* est également présent. Il est constitué de nombreuses informations provenant de la base *OCDE*. Pour chaque pays, chaque secteur d'activités et chaque année, la base fournit une valeur illustrant différents champs, comme le chiffre d'affaire, le nombre total d'employés, ou encore les salaires moyens. Le dernier fichier, *valueadd.csv* est la valeur ajoutée entre chaque secteur d'activités (et sous-secteur d'activités) en 2015. Toutes ces informations sont brutes et un script permet de retraiter ces informations.

Le dossier *DatabaseAprès* est composé de deux fichiers de type *csv*. Le premier est *ocde.csv* et est une source d'information sur le chiffre d'affaires, le nombre d'entreprises et d'employés par secteur d'activités étudié ici. Elle a été créée grâce à la conversion de monnaie (tout en euro) et grâce au fichier *turnover.csv*. Le second est *valueadd.csv* est une sous base de données du fichier du même nom dans le dossier *Databaseavant*. Il comporte la même information, mais retraité pour les secteurs d'activités qui sont présent dans l'application.

Enfin, quatre scripts R sont présents à la racine du dossier de l'application :

— **Retreatment.R :** Ce script contient tout le retraitement effectué sur les bases de données. Il permet donc la création des fichiers dans *DatabaseAprès* à partir des fichiers de *DatabaseAvant*. Fondamentalement, il n'est pas nécessaire au fonctionnement de l'application, mais permet de mieux comprendre la façon dont le retraitement a été effectué,

— **Main.R :** Ce script est le plus cruciale de l'application. Il permet de réaliser la modélisation de la propagation du rançongiciel. Il comporte plusieurs fonctions permettant d'intégrer tous les paramètres présentés lors du chapitre 5. Toutes ces fonctions seront détaillées dans une sous-section suivante,

— **Ui.R** : Ce script permet de créer toute la partie graphique de l'application. Il informe du positionnement des éléments, du texte, ou encore de la couleur. C'est un peu l'équivalent des fichiers *HTML/CSS* pour la création de site,

— **Server.R :** Ce script est nécessaire au fonctionnent du *Rshiny*. Il permet de faire la passerelle entre la partie visuelle (*Ui.R*) et les fonctions du script *Main.R*.

B.0.2 Packages nécessaires et version de R

La version de R utilisée pour la réalisation de cette application est la 4.1.0. Logiquement, elle devrait fonctionner sur les versions plus récentes. L'architecture est en 64 bits, mais ne devrait pas poser de problème en 32 bits. Enfin, les packages nécessaires et les versions associées au lancement de l'application sont les suivants :

Package	Version
data.table	1.14.0
gtools	3.9.2
ggplot2	3.3.4
shiny	1.7.1
shinyFiles	0.9.1
shinythemes	1.2.0
shinyWidgets	0.6.3
rmarkdown	2.9
shinycssloaders	1.0.0
RColorBrewer	1.1
gridExtra	2.3
deSolve	1.28

Une version plus récente de ces packages ne devraient pas poser de problème lors du lancement de l'application. Cependant, à l'avenir, certains packages peuvent ne plus être installés depuis R si le site `https://cran.r-project.org/` décident de ne plus fournir ces éléments pour une raison externe. Enfin R peut être capricieux et empêcher le fonctionnement de l'application à cause des dépendances des packages. Certains d'eux peuvent être remplacés et comme le code est open source, libre à chacun de modifier l'application pour remplacer certains packages.

B.0.3 Lancement de l'application

Après avoir installé les packages mentionnés ci-dessus, il est nécessaire d'ouvrir avec Rstudio le script *Ui.R* ou *Server.R*. Une fois ouvert, un bouton *Run App* est présent sur la barre de la fenêtre du script (cf la figure suivante)

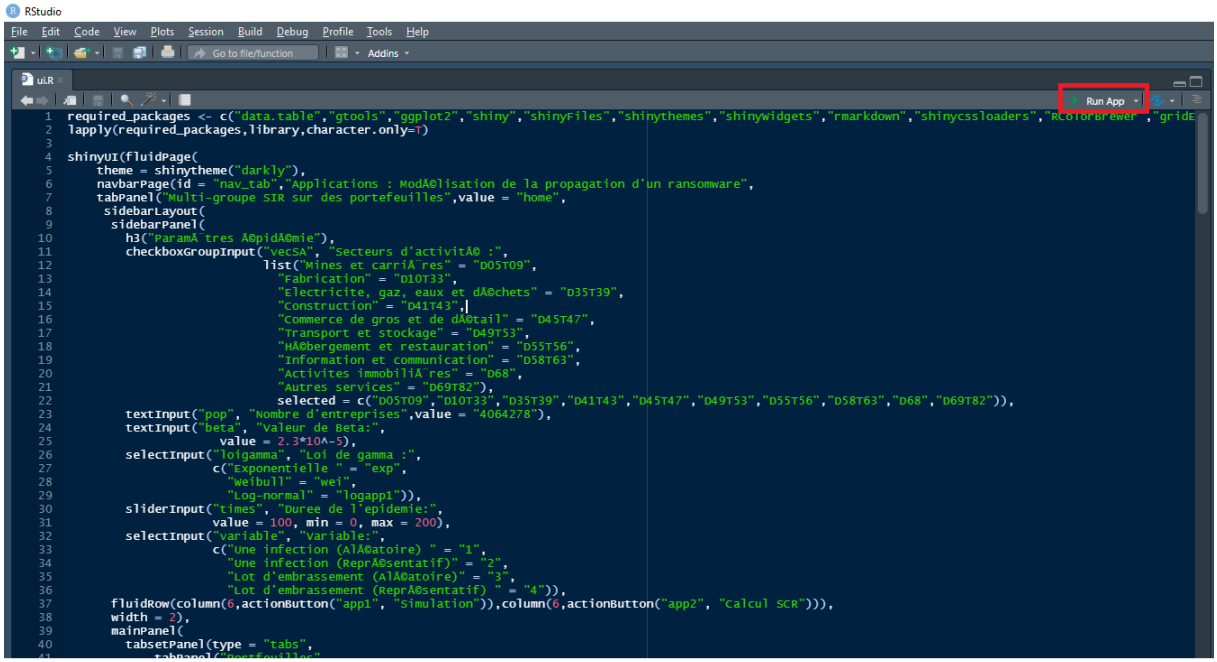

FIGURE B.2 – Localisation du bouton *Run App* permettant de lancer l'application

En cliquant sur ce bouton-là, l'application se lance. Comme présenté dans le chapitre 5, l'utilisateur obtient une nouvelle fenêtre avec le visuel de la figure 5.5 *L'application Rshiny permettant de tester*

différents paramètres pour la propagation d'un rançongiciel à travers trois portefeuilles.

Fonctionnement du code

Parmi les 4 scripts R, seul *Main.R* est décrit dans cette annexe. Il comporte toute la partie de calibration, de modélisation et du calcul des impacts des sinistres. Les scripts *Main.R* et *Ui.R* permettent d'afficher la fenêtre Rshiny. De nombreuses documentations sont disponibles sur Internet expliquant exactement comment ces scripts fonctionnent. Le script *Retreatment.R* permet d'obtenir les fichiers présents dans le dossier *DatabaseApres* en utilisant les fichiers du dossier *DatabaseAvant*. La manière dont ce retraitement est effectué a été décrite dans le chapitre 5 lors de la section *Calibration* permet de comprendre l'essence du code qui ne compte qu'une seule fonction réalisant la totalité du retraitement. De plus, de nombreux commentaires sont présents indiquant l'objectif de chaque étape.

Le fichier *Main.R* comporte 17 fonctions réalisant la récupération des paramètres calibrés jusqu'à l'exécution de plus de 50000 scénarios. Deux fonctions peuvent être lancées depuis l'application. Elles vont appeler toutes les autres fonctions afin de réaliser le travail demandé. Ces deux fonctions sont *simulation* et *calculscenario*. Elles sont quasiment identiques, à la différence que :

— la première réalise une seule simulation et apporte les éléments de la figure 5.7 et de la figure 5.8 (autrement dit les graphiques affichés dans les onglets *Graphique infection* et *Graphique portefeuille*),
— la seconde effectue 50000 simulations du scénario demandé, en utilisant uniformément les différentes possibilités proposées (loi du taux de guérison et début de l'épidémie).

Les arguments nécessaires au fonctionnement des deux fonctions sont :
— *vecSA :* Les codes *OCDE* correspondant aux secteurs d'activités choisis,
— *Npop :* Le nombre correspondant à la population globale,
— *beta :* La valeur du taux de transmission,
— *loigamma :* La loi du taux de guérison,
— *times :* La durée de l'épidémie,
— *choix :* La manière dont l'épidémie débute,
— *pf :* La taille des portefeuilles,
— *CountryportC :* Liste des pays composant le portefeuille C,
— *SAportC :* La composition du portefeuille C selon les secteurs d'activités.

À noter que tous le code, même la partie modélisation et résolution des équations différentielles, ainsi que la création des graphiques s'adaptent au nombre de secteurs d'activités initialement choisies.

La première fonction appelait est *Ajoutsophostouchcouvert* qui permet d'ajouter les statistiques de Sophos sur le pourcentage des secteurs d'activités touchés par un rançongiciel, ainsi que le pourcentage des secteurs d'activités touchées.Les secondes et troisièmes fonctions utilisées sont *globalocde* et *paysocde* et permettent de récupérer toutes les informations sur les secteurs d'activités et les pays. Ces informations sont concaténées dans des data frames.

La fonction suivante *CalculMatriceBeta* permet de calibrer la matrice B et probabilise la loi de γ. Toutes ces étapes sont décrites dans la section *Calibration* et reproduit exactement ce qui a été énoncé. Ensuite, un vecteur composé des paramètre nécessaire au fonctionnement de la résolution des équations différentielles est obtenue via la fonction *NormalizationByAll*. Il est également appliqué le taux de transmission à la matrice B.

Le choix du début de l'épidémie est ensuite choisi dans la fonction *ignitepf* qui permet d'obtenir le nombre d'individus présent dans chaque compartiment du modèle SIR (les compartiments sains, infectés et guéris). Ce nouveau vecteur alimente la fonction *calculout* qui résout les équations

différentielles. Provenant du package *deSolve*, la fonction *ode* est spécialisée dans la résolution d'un système d'équations différentielles ordinaires. En lui fournissant, l'état de départ des compartiments, la fonction *sirmg2* qui contient les équations différentielles présentées lors du chapitre 2 sur le modèle multi-groupes SIR, il est obtenu l'évolution du nombre d'individus dans chaque compartiment. Bien entendu, cette fonction s'adapte en amont au nombre de secteurs d'activités fournis, i.e. le nombre de groupes du modèle SIR. La fonction *f1* permet d'obtenir le graphe de la figure 5.7.

La fonction suivante permet de calculer la taille finale de l'épidémie en utilisant la formule démontré lors de la sous-section suivante *La taille finale d'une épidémie d'un modèle multi-groupes* qui est :

$$F_k(X) = S_k(0) * \exp\left(\sum_{j=1}^{n} \frac{\beta_{kj}}{\gamma_j}(X_j - S_j(0)) - \sum_{j=1}^{n} \frac{\beta_{kj}}{\gamma_j} I_j(0)\right)$$

Enfin les derniers fonctions nommées respectivement *PortA*, *PortB* et *PortC*, permettent de calculer d'après l'évolution du nombre d'individus dans chaque compartiment obtenue par la fonction *ocde* le nombre d'assurés touchés ainsi que le coût par secteur d'activités et par pays. La fonction *f2* conclut en affichant les graphiques de la figure 5.8.

À noter que pour la fonction *calculscenario* est parallélisé. Ce terme signifie que tous les cœurs du processeur vont être mis à disposition afin de réaliser plus rapidement le xs simulations (puisque de base un seul cœur est alloué à R). Le temps de calcul étant de 1h pour 50000 simulations, le gain de temps obtenu par la simulation correspond à un temps diminué par 3. Afin d'accélérer la vectorisation des boucles en compilant les octets, les fonctions ont toutes une interface à un compilateur de code d'octet pour R via la fonction *cmpfun*.

Détails des simulations

Les figures suivantes récapitulent le résultat des 50 000 simulations pour chaque loi γ et choix du début de l'épidémie utilisés. Le paramètre du taux de transmission β est de 2.3, tout comme dans le scénario présenté dans le chapitre 5 :

	Value	Portefeuille A	Portefeuille B	Portefeuille C
Exponentielle	Min	0,00 €	0,00 €	0,00 €
	Moyenne	1 412,30 €	1 576,15 €	446,04 €
	Mediane	1 654,46 €	1 452,07 €	462,75 €
	Ecart-type	596,26 €	918,24 €	201,00 €
	SCR	2 150,56 €	4 006,08 €	825,79 €
	Max	2 160,86 €	6 104,39 €	832,92 €
Weibull	Min	0,00 €	0,00 €	0,00 €
	Moyenne	945,05 €	1 065,25 €	246,32 €
	Mediane	933,86 €	877,46 €	239,57 €
	Ecart-type	607,89 €	847,90 €	171,68 €
	SCR	2 031,51 €	3 508,11 €	688,40 €
	Max	2 152,04 €	4 781,25 €	827,16 €
Log Normal	Min	0,00 €	0,00 €	0,00 €
	Moyenne	956,64 €	1 074,12 €	251,31 €
	Mediane	955,58 €	885,83 €	246,28 €
	Ecart-type	623,90 €	862,51 €	175,48 €
	SCR	2 041,70 €	3 551,65 €	692,11 €
	Max	2 146,92 €	7 168,96 €	823,98 €

FIGURE B.3 – Simulations : Détails des différentes informations en termes de coût totale des sinistres sur les 50 000 simulations réalisées pour les 3 lois. Le coût est exprimé en millions.

	Value	Portefeuille A	Portefeuille B	Portefeuille C
1 infection (aléatoire)	Min	0,00 €	0,00 €	0,00 €
	Moyenne	1 064,45 €	1 186,12 €	297,24 €
	Mediane	1 092,91 €	1 017,14 €	288,52 €
	Ecart-type	642,08 €	897,24 €	199,84 €
	SCR	2 130,51 €	3 699,50 €	796,23 €
	Max	2 160,28 €	5 975,57 €	832,48 €
1 infection (représentative)	Min	0,00 €	0,00 €	0,00 €
	Moyenne	1 065,54 €	1 188,68 €	297,80 €
	Mediane	1 089,80 €	1 020,61 €	288,79 €
	Ecart-type	641,76 €	894,22 €	200,52 €
	SCR	2 134,07 €	3 706,58 €	796,97 €
	Max	2 160,28 €	4 980,24 €	832,48 €
Lot d'embrasement (aléatoire)	Min	2,55 €	1,74 €	1,63 €
	Moyenne	1 061,19 €	1 203,21 €	297,27 €
	Mediane	1 084,01 €	1 029,09 €	287,50 €
	Ecart-type	642,48 €	897,16 €	199,92 €
	SCR	2 134,15 €	3 738,11 €	796,27 €
	Max	2 160,83 €	5 716,24 €	832,86 €
Lot d'embrasement (représentatif)	Min	1,85 €	1,05 €	1,19 €
	Moyenne	1 062,84 €	1 185,81 €	297,44 €
	Mediane	1 087,58 €	1 018,92 €	288,25 €
	Ecart-type	642,01 €	895,76 €	200,00 €
	SCR	2 130,46 €	3 700,45 €	793,90 €
	Max	2 159,93 €	5 702,58 €	832,42 €

FIGURE B.4 – Simulations : Détails des différentes informations en termes de coût totale des sinistres sur les 50 000 simulations réalisées pour les 4 choix de début d'épidémie. Le coût est exprimé en millions.