RISQUE CYBER, UN MODÈLE ÉPIDÉMIOLOGIQUE SUR RÉSEAUX POUR LE RISQUE D'ACCUMULATION DU CYBER SILENCIEUX

Thomas Peyrat

Le 5 octobre 2023

4, rue Chauveau-Lagarde – 75008 Paris – tél. 01 44 51 72 72
www.institutdesactuaires.com

Institut des ACTUAIRES

SOMMAIRE

1 Le risque cyber

2 Le risque d'accumulation du cyber silencieux

3 Application du modèle à un portefeuille fictif

4 Des mesures à prendre

SOMMAIRE

1 Le risque cyber

A Introduction

B Contexte et problématique

INTRODUCTION

“Une **cyber-attaque** est une atteinte à des **systèmes informatiques** réalisée dans un but **malveillant**. Elle cible différents dispositifs informatiques : des ordinateurs ou des serveurs, isolés ou en réseaux, reliés ou non à Internet, des équipements périphériques tels que les imprimantes, ou encore des appareils communicants comme les téléphones mobiles, les ≪ smartphones ≫ ou les tablettes.”

Plusieurs types d’attaques

Dans des domaines différents

- Cybercriminalité
- L’atteinte à l’image
- L’espionnage
- Le sabotage

Un environnement juridique

Et institutionnel dynamique

- CNIL / ANSSI / ENISA
- NIS -> NIS2
- Devons-nous payer les rançons ?
- Un aléa juridique sur les clauses d’exclusions

Une modélisation actuarielle

Qui pose plusieurs défis

- Une composante systémique
  - Autocorrélation des évènements
  - Effet d’accumulation
- Des sinistres extrêmes
- Un manque de données

LES ÉLÉMENTS TRAITÉS

Les rançongiciels

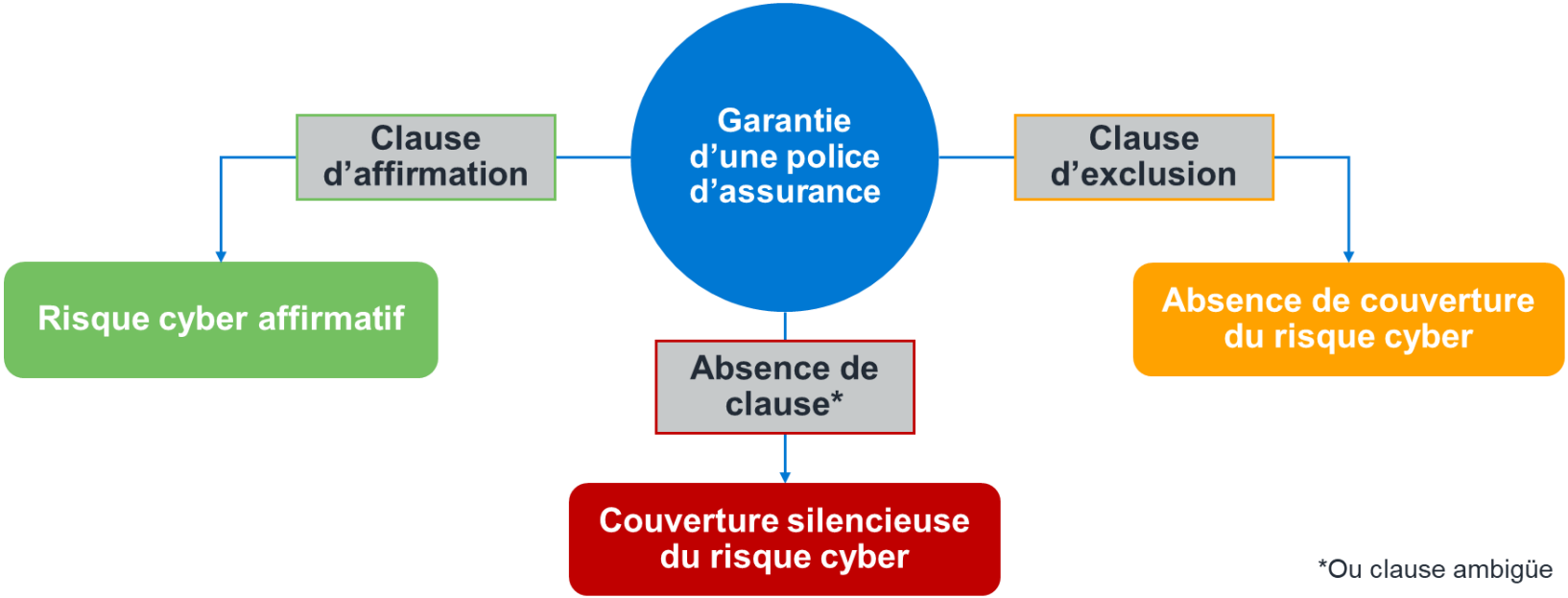
Le cyber silencieux

L'effet d'accumulation

LES RANÇONGICIELS

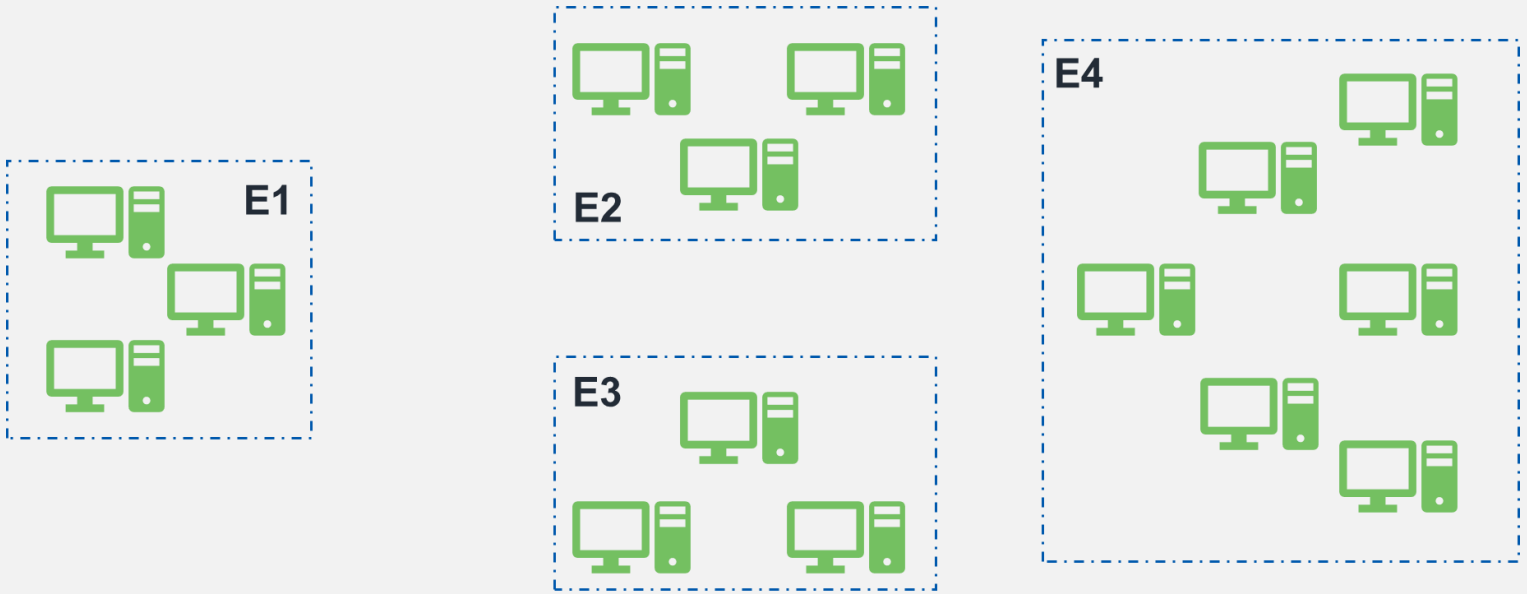
- Exemple du rançongiciel Wannacry en 2017

LE CYBER SILENCIEUX

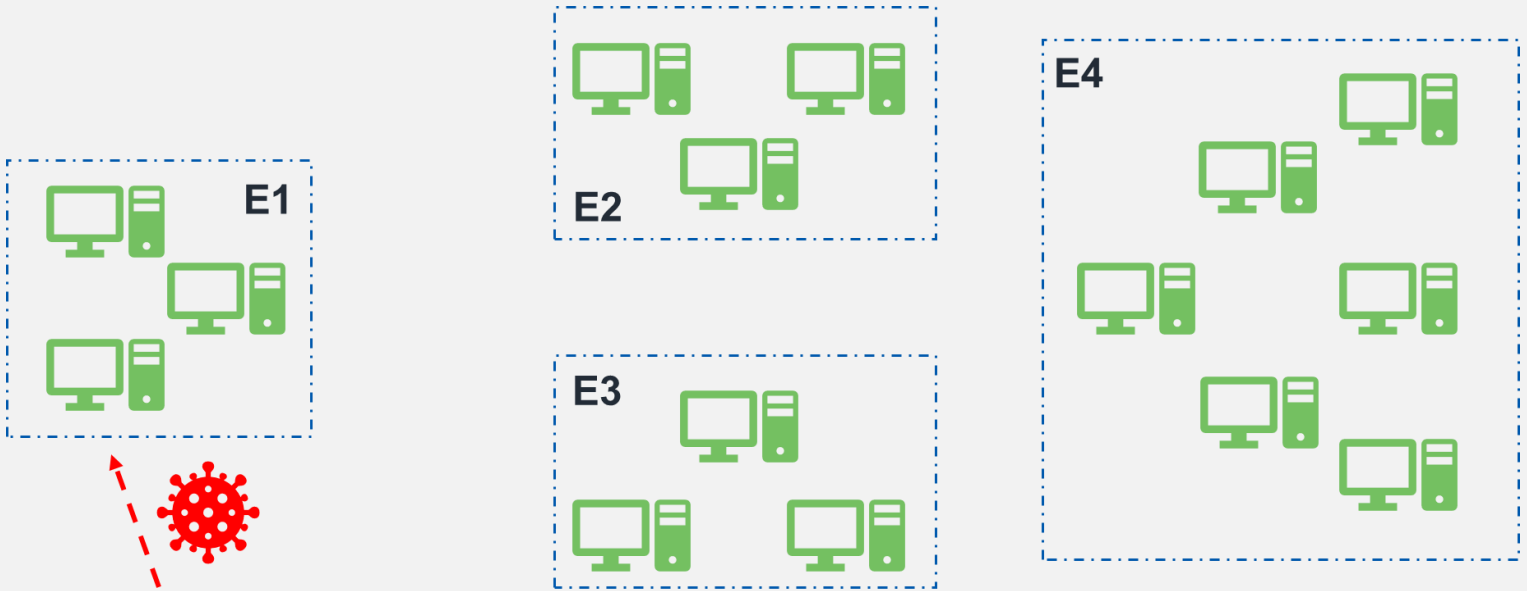


*Ou clause ambigüe

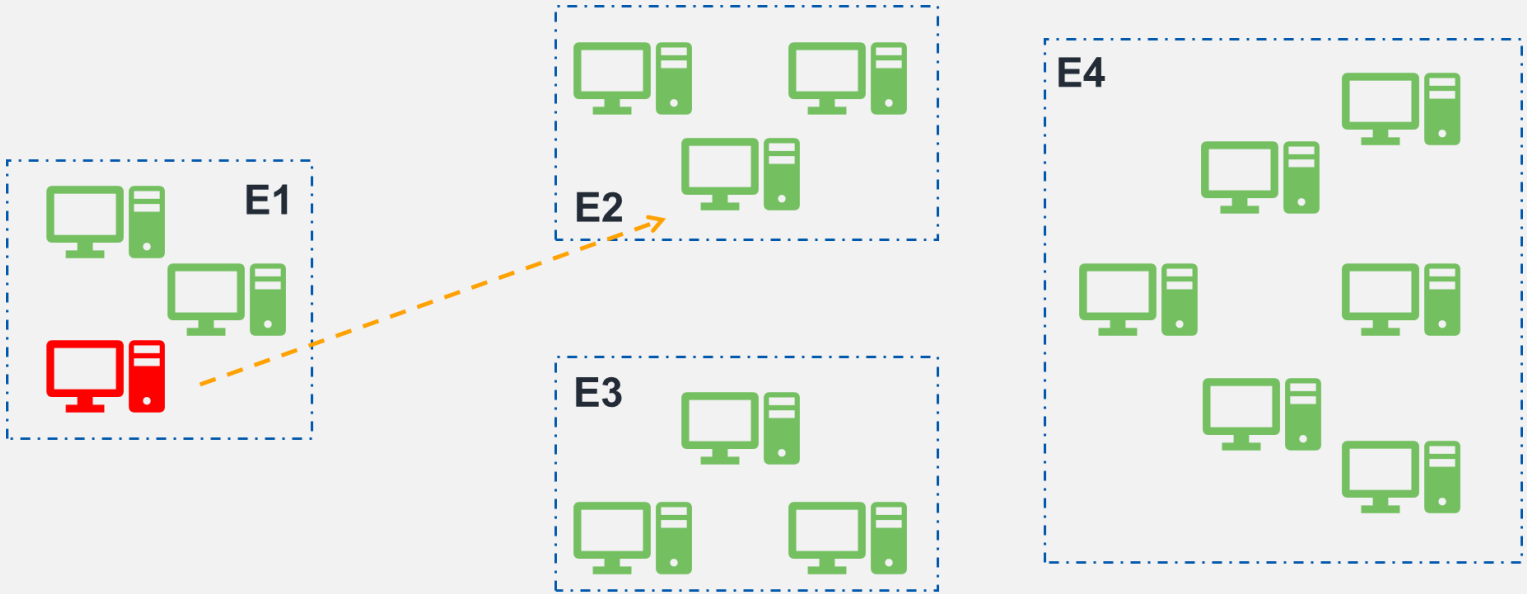
L'EFFET D'ACCUMULATION



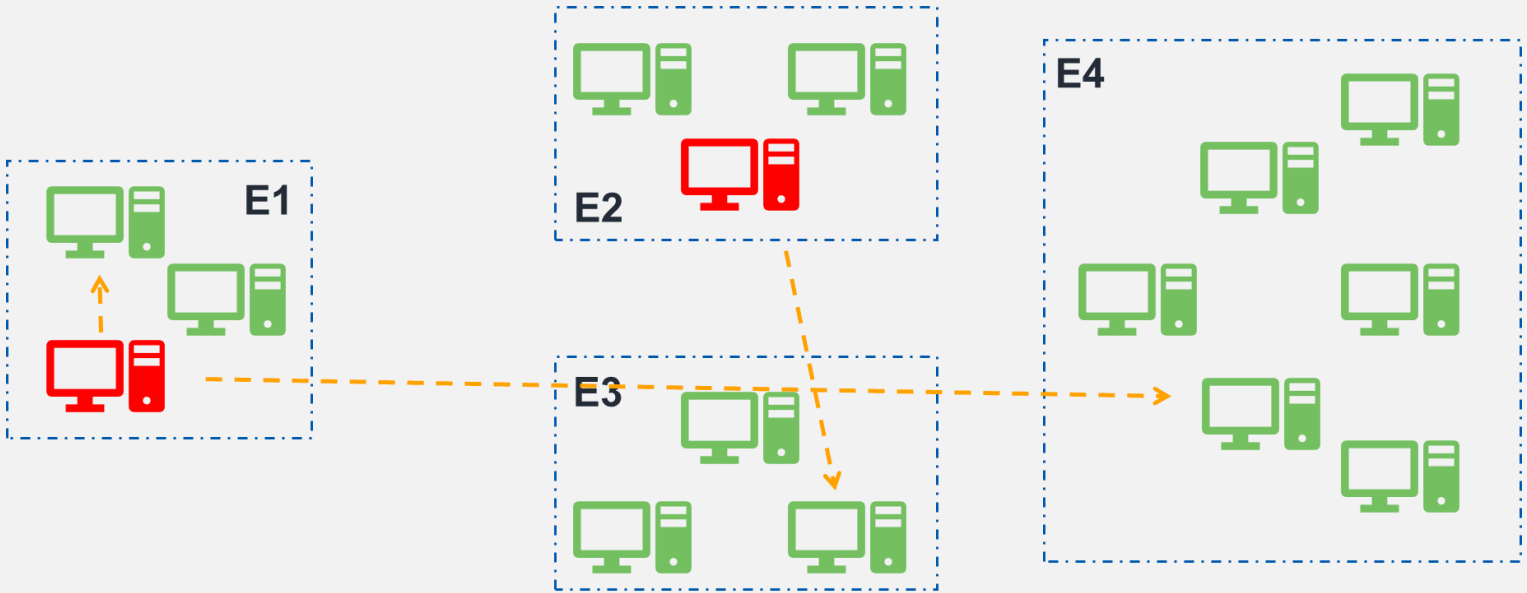
L'EFFET D'ACCUMULATION



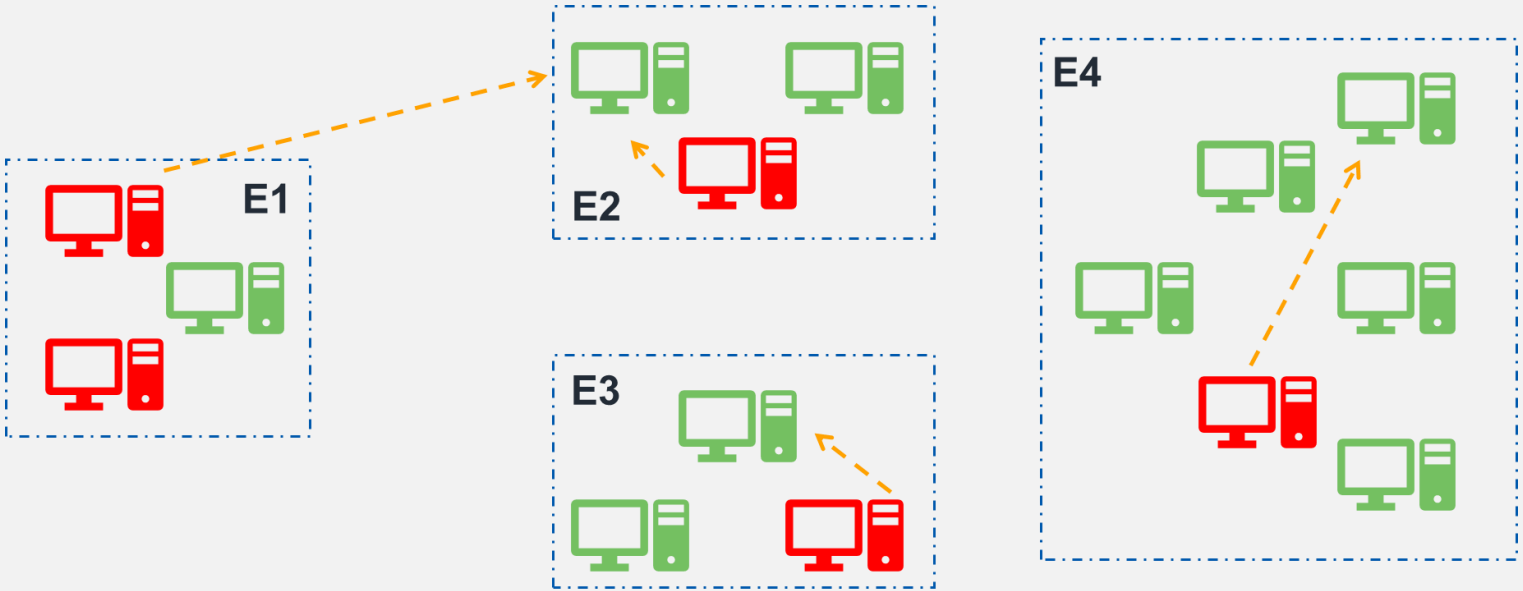
L'EFFET D'ACCUMULATION



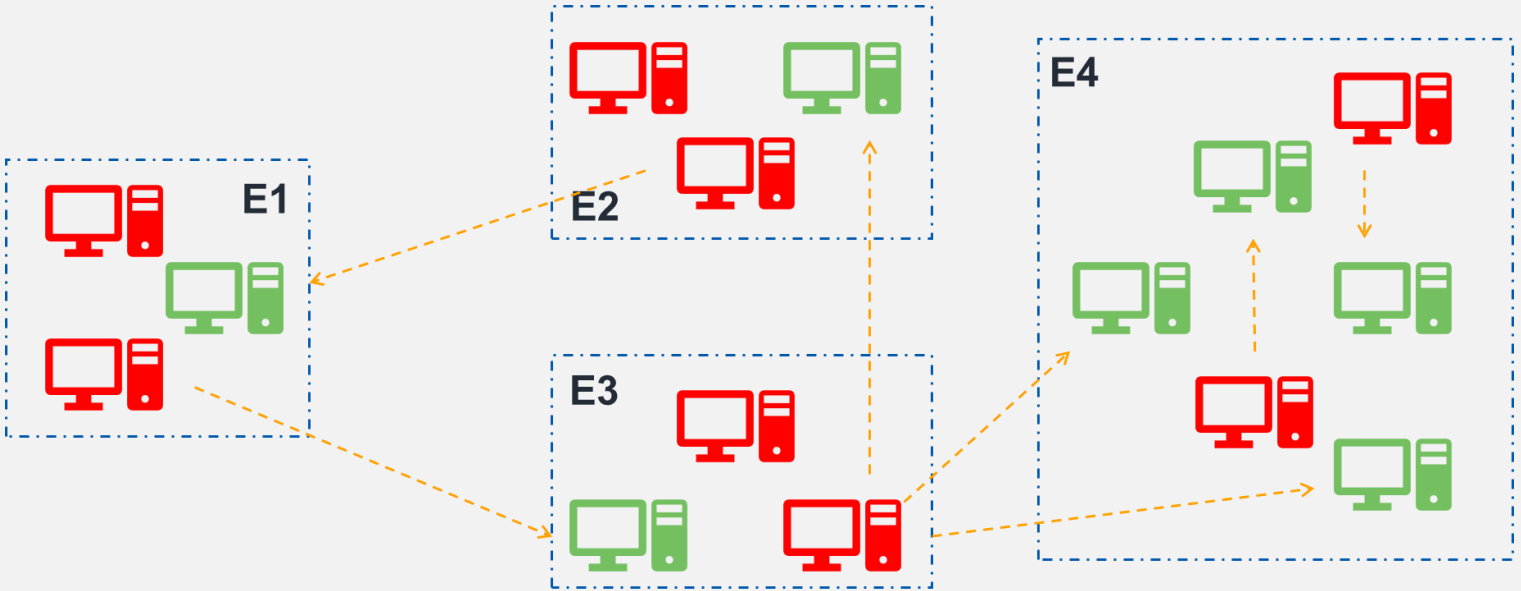
L'EFFET D'ACCUMULATION



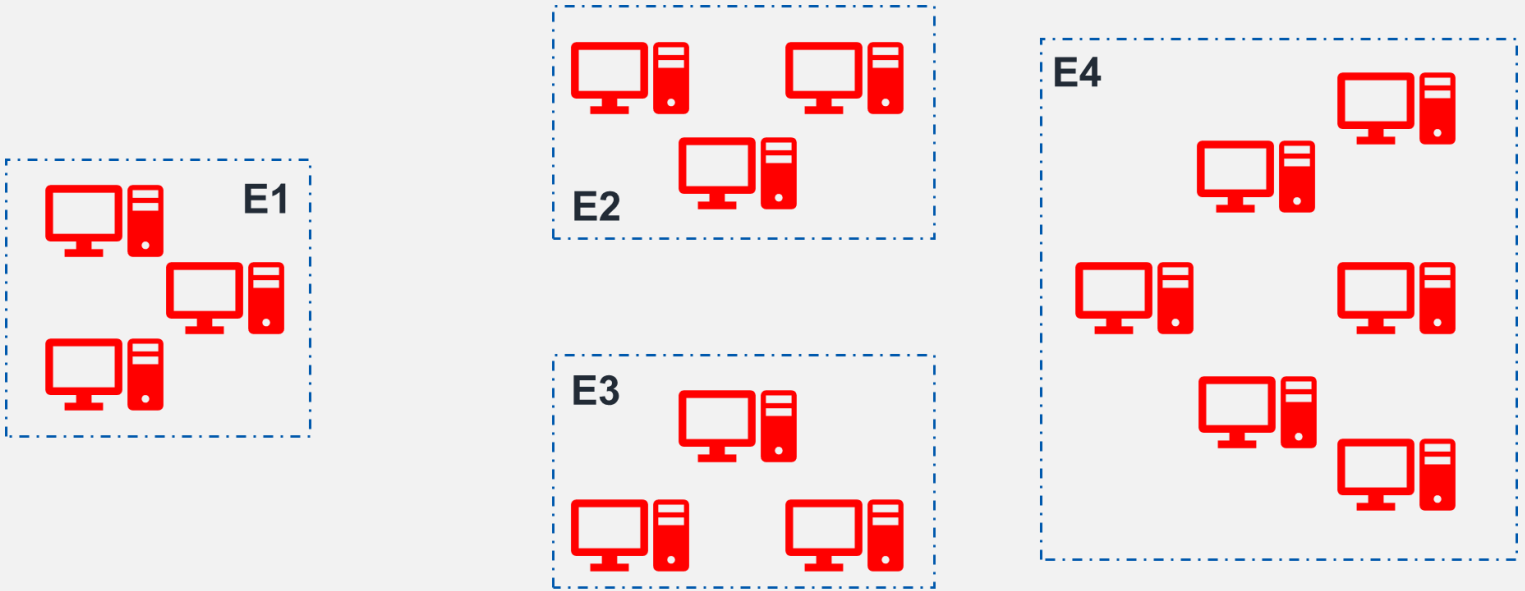
L'EFFET D'ACCUMULATION



L'EFFET D'ACCUMULATION



L'EFFET D'ACCUMULATION



PROBLÉMATIQUE

L'impact de la prise en compte du risque d'accumulation cyber sur la résilience des portefeuilles non-cyber:

Comment modéliser le phénomène d'accumulation pour l'appliquer au cas du cyber silencieux ?

Institut des ACTUAIRES

SOMMAIRE

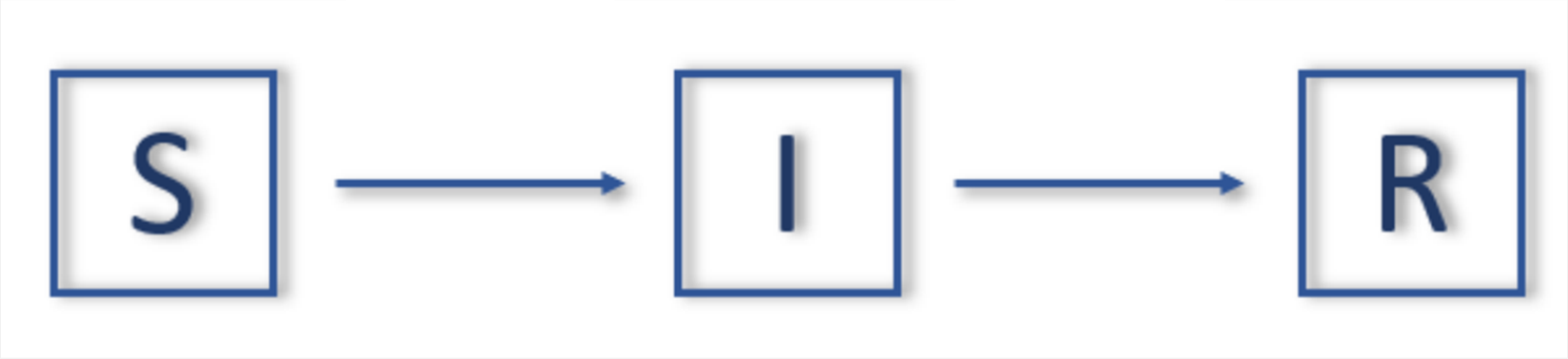
2 Le risque d'accumulation du cyber silencieux

A Les modèles compartimentaux

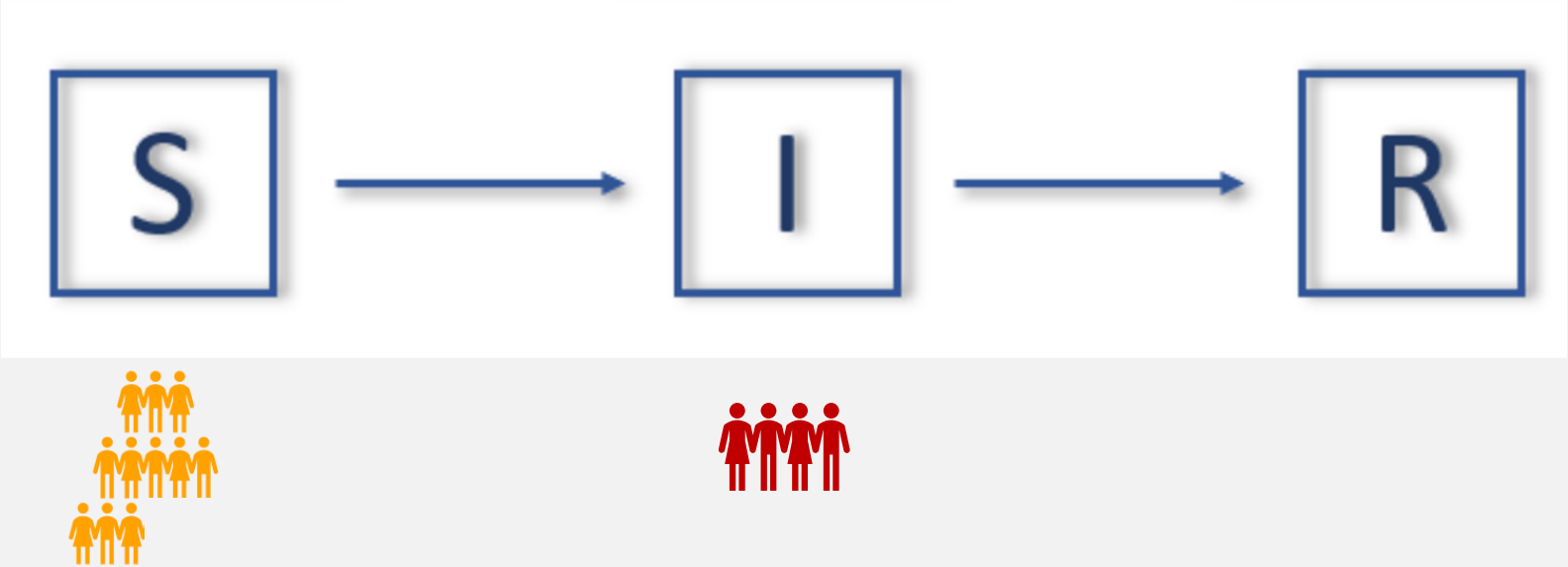
B Prise en compte de l'hétérogénéité via des réseaux

C Modélisation des pertes silencieuses

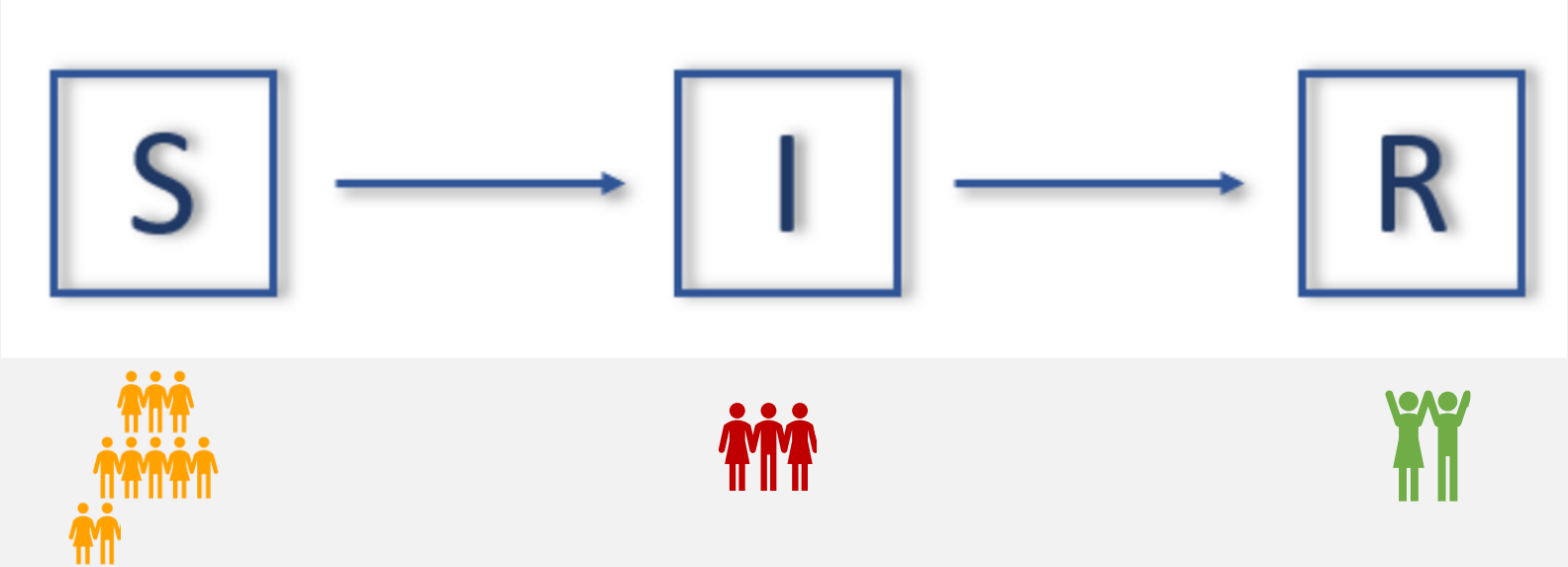
LES MODÈLES COMPARTIMENTAUX



LES MODÈLES COMPARTIMENTAUX



LES MODÈLES COMPARTIMENTAUX



Nombre de susceptibles

Taux d'infection

$$\frac{dS(t)}{dt} = -\beta I(t)\frac{S(t)}{N},$$

Taux de rétablissement

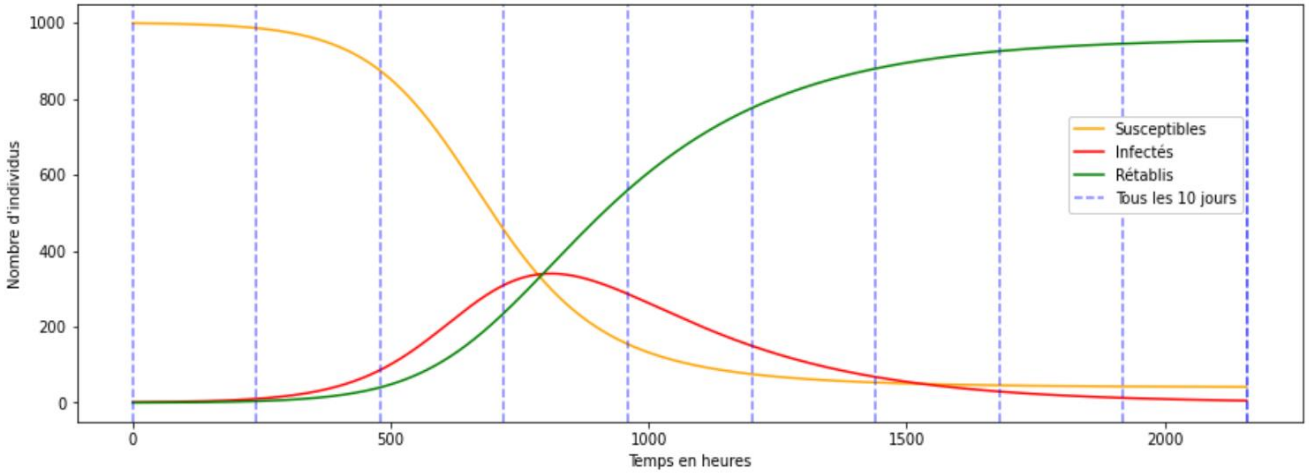
Nombre d'infectés

$$\frac{dI(t)}{dt} = \beta I(t)\frac{S(t)}{N} - \gamma I(t),$$

Nombre de rétablis

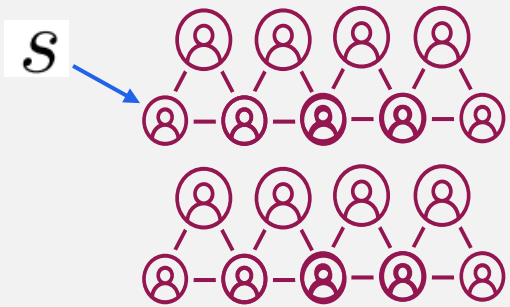
Nombre d'individus

$$\frac{dR(t)}{dt} = \gamma I(t).$$



Exemple de trajectoires pour le modèle SIR.

$$\frac{dS(t)}{dt} = -\beta I(t)\frac{S(t)}{N},$$
$$\frac{dI(t)}{dt} = \beta I(t)\frac{S(t)}{N} - \gamma I(t),$$
$$\frac{dR(t)}{dt} = \gamma I(t).$$



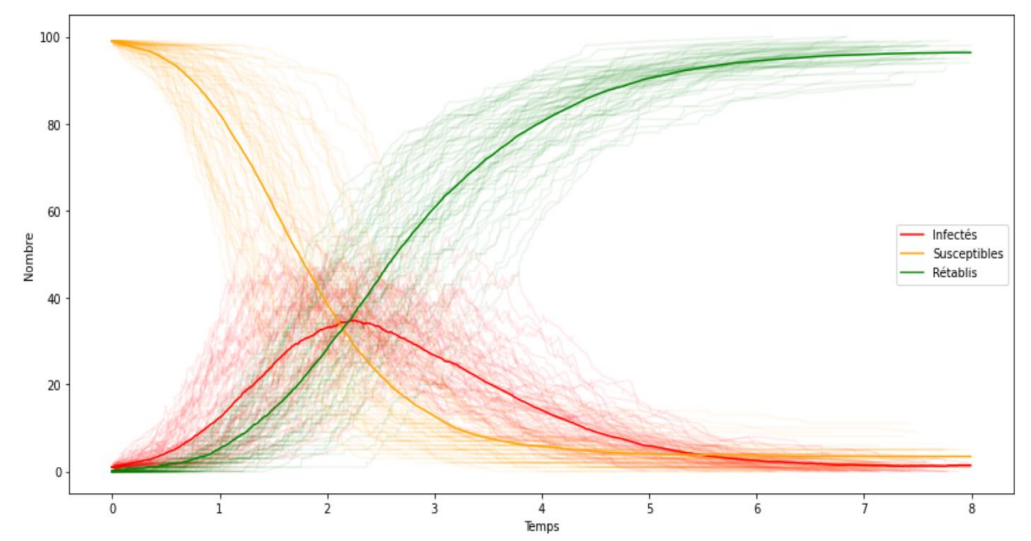
$E_s(t) \in \{S, I, R\}$ Etat du nœud → S

Matrice d'adjacence

$$E_{s_i}(t) : S \to I \quad \text{avec un taux} \quad \beta \sum_{s_j \in S} a_{ij} \mathbb{1}_{E_{s_j}(t)=I},$$

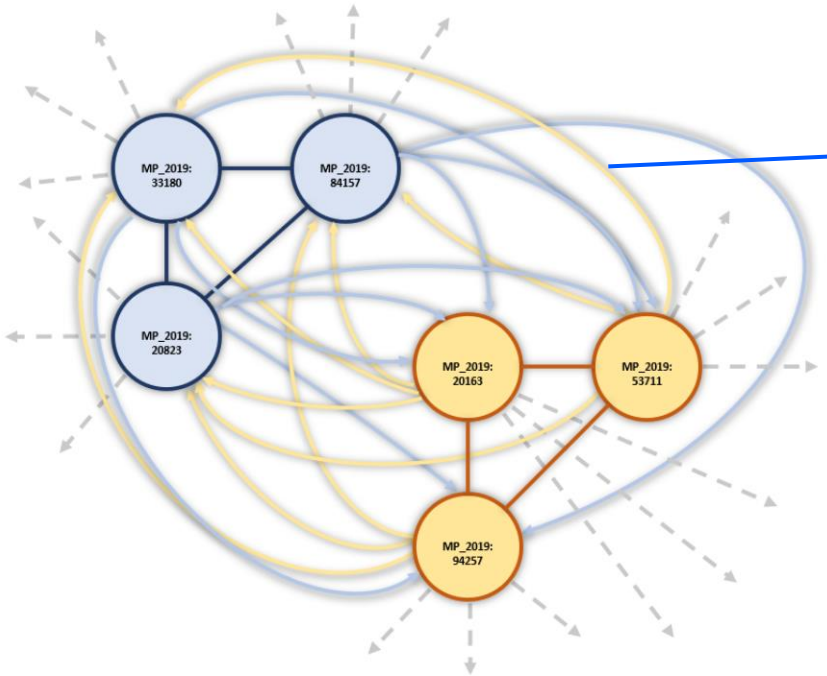
$$E_{s_i}(t) : I \to R \quad \text{avec un taux} \quad \gamma.$$

- L'information du réseau est contenue dans la matrice d'adjacence
- Le taux d'infection d'un individu dépend du nombre d'infecté autour de lui
- Le taux de rétablissement est indépendant de la structure de réseau



Exemple de trajectoires pour le nouveau modèle SIR.

- Le modèle est maintenant stochastique
- Plusieurs simulations sont nécessaires pour obtenir une trajectoire moyenne

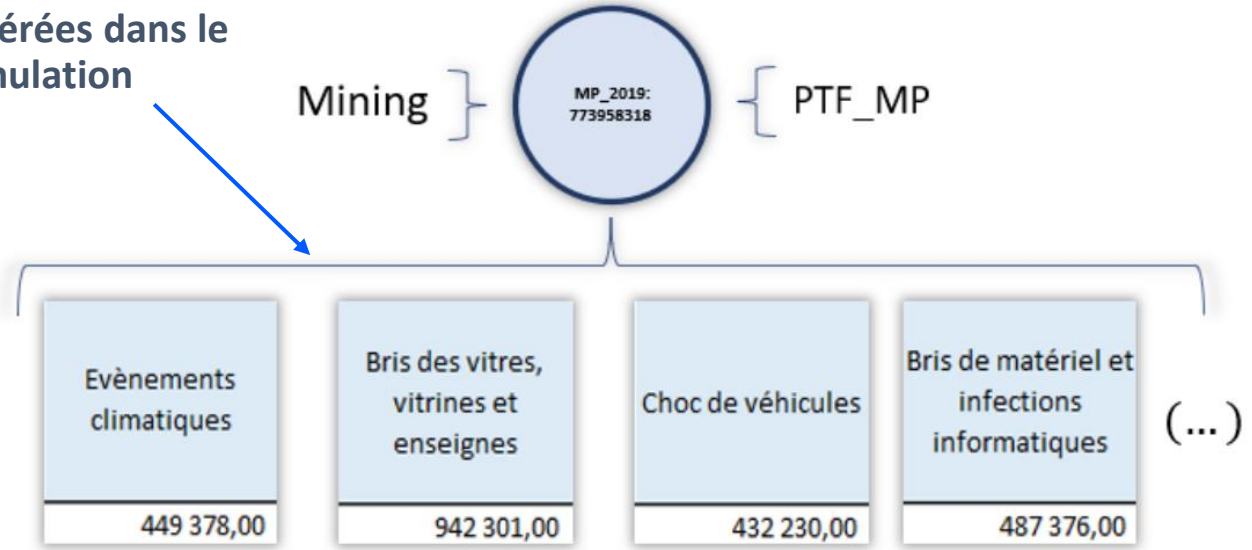


$$E_{s_i}(t) : S \to I \quad \text{avec un taux} \quad \beta \sum_{s_j \in S} a_{ij} \mathbb{1}_{E_{s_j}(t)=I},$$

$$E_{s_i}(t) : I \to R \quad \text{avec un taux} \quad \gamma.$$

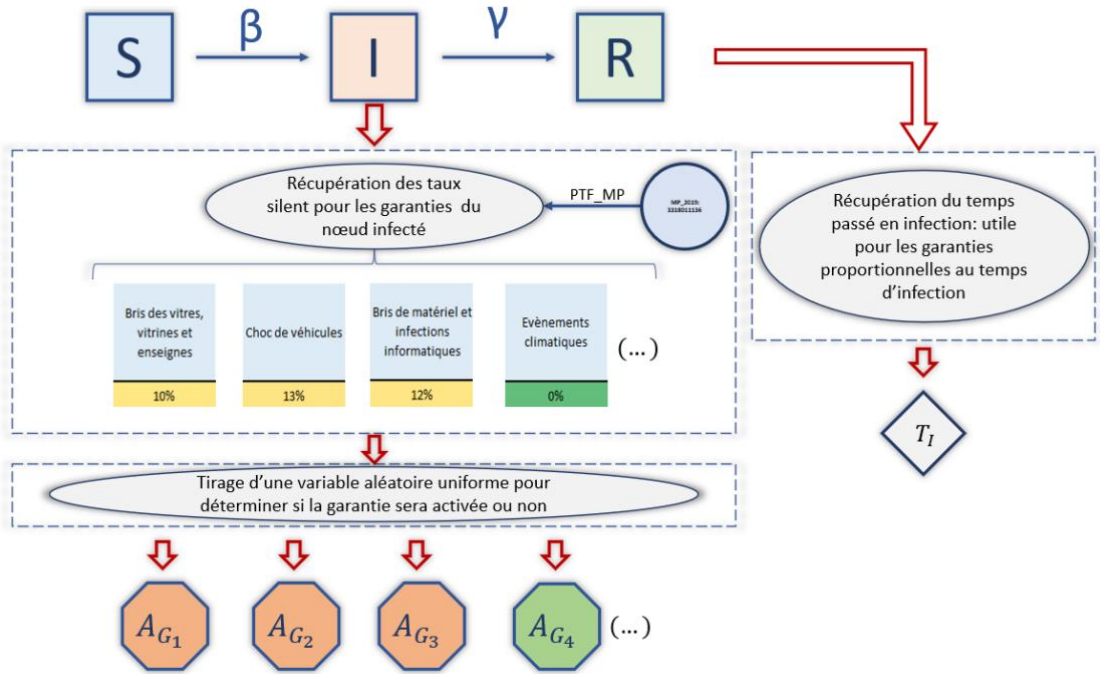
- Le graphe est orienté et possède des poids sur ses arcs
- L'information des poids est contenue dans la matrice d'adjacence
- Les nœuds du réseau représentent les assurés

Garanties considérées dans le scénario d'accumulation



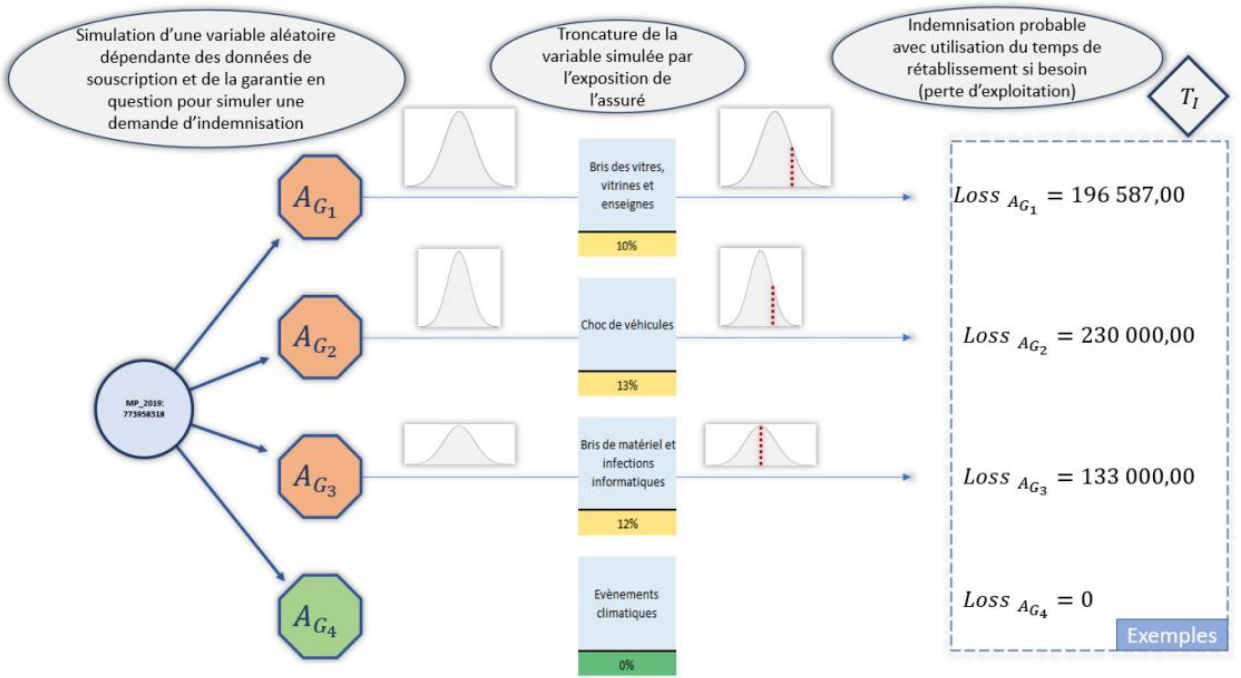
Informations contenues dans un nœud représentant l'assuré.

C – Modéliser les pertes silencieuses



Processus d'activation des garanties sur le modèle SIR.

- Il est impératif de maintenir une cohérence entre les pertes simulées et l'exposition
- Une modélisation au cas par cas peut être à considérer pour certaines garanties
- Cette modélisation dépendra des données disponibles chez les assureurs



Processus de génération d'une perte pour les garanties d'un nœud infecté.

Institut des ACTUAIRES

SOMMAIRE

3 Application a un portefeuille fictif

A Construction du portefeuille

B Les hypothèses du scénario

C Premiers résultats

Matrice des garanties possibles par produit		Locaux et leur contenu											
Produits	**Libellé**	Tempête	Grêle	Avalanche, poids de la neige, gel, inondation	Evènements climatiques	Bris des vitres, vitrines et enseignes	Choc de véhicules	Dommages amménagements extérieurs	Vol hors domicile	Vol tentative de vol et vendalisme	Perte du contenu des congélateurs et caves à vin	Bris de matériel	Bris de matériel et infections informatiques
MP_2022	ASSURANCE MULTIRISQUE PROFESSIONNELS				1	1	1	2		2		2	
MBTP_2022	ASSURANCE MULTIRISQUE DES PROFESSIONNELS DU BÂTIMENTET DES TRAVAUX PUBLICS				1	1	1	2		2		2	
MRH:Init_2012	ASSURANCE MULTIRISQUE TEMPO HABITATION : Initiale	1	1			1	1			1			
MRH:Clas_2012	ASSURANCE MULTIRISQUE TEMPO HABITATION : Classique	1	1			1	1			1			
MRH:Full_2012	ASSURANCE MULTIRISQUE TEMPO HABITATION : Intégrale	1	1	1		1	1		1	1	1		

Extrait de la matrice des garanties par produits.

- Cette matrice a été construite à partir de conditions générales disponibles sur internet
- Elle permet de générer des portefeuilles de polices d'assurance représentatives du marché

Multirisques Professionnels	Information de souscription											
No_Contrat	Secteur	Grêle	Avalanche, poids de la neige, gel, inondation	Evènements climatiques	Bris des vitres, vitrines et enseignes	Choc de véhicules	Dommages amménagements extérieurs	Vol hors domicile	Vol tentative de vol et vendalisme	Perte du contenu des congélateurs et caves à vin	Bris de matériel	Bris de matériel et infections informatiques
Taux Silent -->		0%	0%	0%	10%	13%	5%	2%	2%	40%	33%	12%
MP_2019: 773958318	Energy	-	-	449 378,00	942 301,00	432 230,00	756 724,00	-	-	-	-	487 376,00
MP_2019: 4477225817	Services	-	-	392 535,00	336 113,00	989 196,00	48 969,00	-	-	-	-	-
MP_2019: 5012578793	Mining	-	-	684 154,00	736 806,00	32 668,00	75 400,00	-	-	-	-	843 571,00
MP_2019: 3920573794	Services	-	-	738 825,00	737 263,00	469 771,00	512 267,00	-	-	-	-	380 360,00
MP_2019: 7029031177	Manufacturing	-	-	682 983,00	658 998,00	466 337,00	-	-	-	-	-	-
MP_2019: 3394212725	Energy	-	-	266 418,00	705 172,00	164 855,00	-	-	12 075,00	-	-	-
MP_2019: 6350782039	Services	-	-	759 542,00	580 677,00	175 646,00	161 031,00	-	-	-	-	-
MP_2019: 5439713871	Services	-	-	613 002,00	588 761,00	586 428,00	-	-	-	-	-	-
MP_2019: 4781945843	Manufacturing	-	-	452 661,00	78 729,00	570 354,00	189 456,00	-	-	-	-	31 882,00
MP_2019: 5163890721	Energy	-	-	209 344,00	241 388,00	656 540,00	-	-	832 130,00	-	-	-

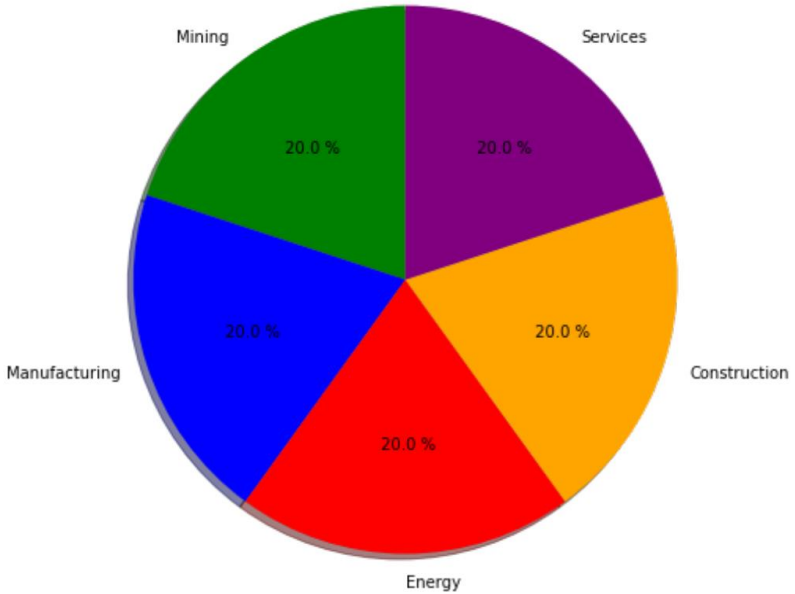
Montants exposés pour les premiers contrats dans le portefeuille Multirisques Professionnels avec les données de souscription et les taux silent.

Multirisque Professionnels	Données de souscription	
No_Contrat	Secteur	Perte d'exploitation
Silent Pourcentage -->		0,32
MP_2019: 3318011136	Mining	150 000,00
MP_2019: 3318011136	Mining	150 000,00
MP_2019: 4903087815	Manufacturing	7 500,00
MP_2019: 4593390988	Manufacturing	7 500,00
MP_2019: 6372174745	Energy	30 000,00
MP_2019: 3315118185	Energy	30 000,00
MP_2022: 3986174666	Construction	15 000,00
MP_2022: 82552042	Construction	15 000,00
MP_2022: 4493508818	Services	15 000,00
MP_2022: 2013765611	Services	15 000,00
(…)		

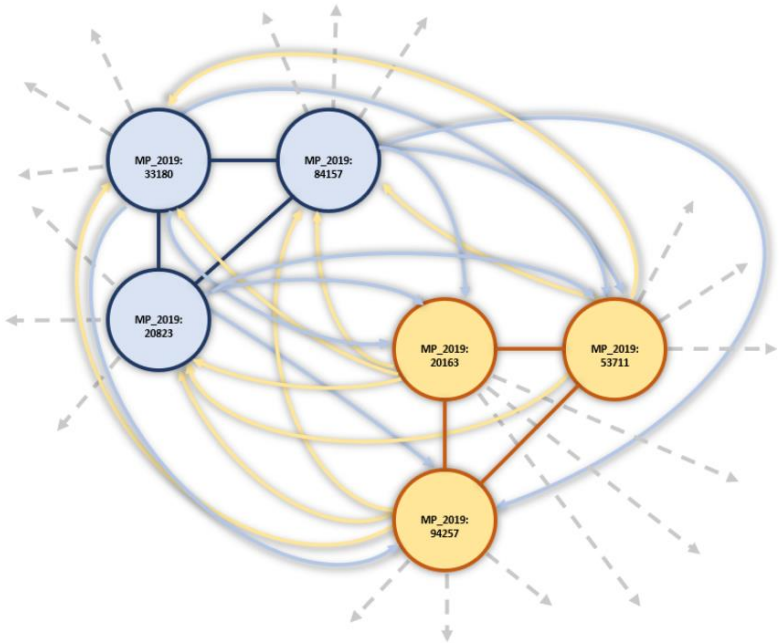
1 000 assurés

- D'après une étude menée par l'AMRAE (LUCY 2022) : **96,2 %** du montant **total indemnisé** provient de « l'assistance gestion de crise / **Pertes d'exploitation** »
- Les expositions représentent les montants maximaux indemnisables par l'assureur sur une journée.
- Les Silent Pourcentage de **0.32** est inspiré du scénario Bashe Attack de l'université de Cambridge
- Chaque entreprise est rattachée à un secteur d'activité

B –Les hypothèses du scénario



Distribution des assurés par secteur d'activité



$$\gamma = 1 \quad \beta = 0.01$$

$$E_{s_i}(t) : S \to I \quad \text{avec un taux} \quad \beta \sum_{s_j \in S} a_{ij} 1_{E_{s_j}(t)=I},$$

$$E_{s_i}(t) : I \to R \quad \text{avec un taux} \quad \gamma$$

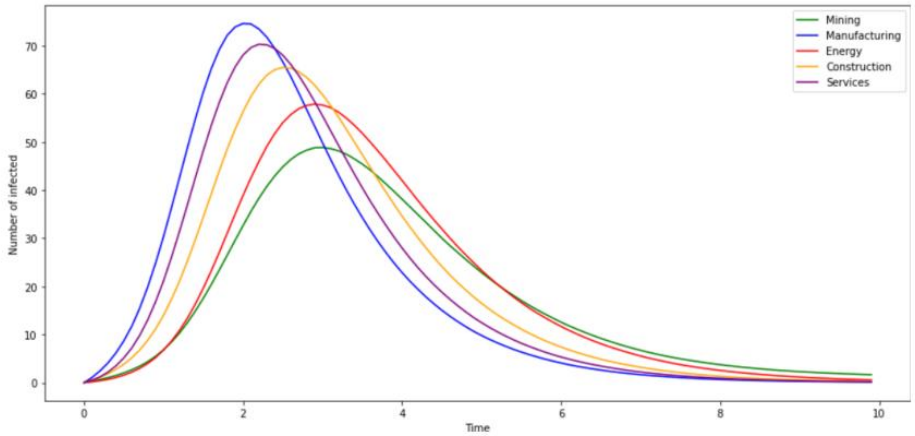
Sectors	Mining	Manufacturing	Energy	Construction	Services
Mining	1	4,61672	0,7082	2,25079	1,9795
Manufacturing	0,0994	0,83123	0,04259	0,17035	0,55363
Energy	0,21293	0,58359	0,90063	0,23659	0,71293
Construction	0,02997	0,10726	0,01104	0,22239	0,14353
Services	0,00473	0,06624	0,00631	0,02681	0,25394

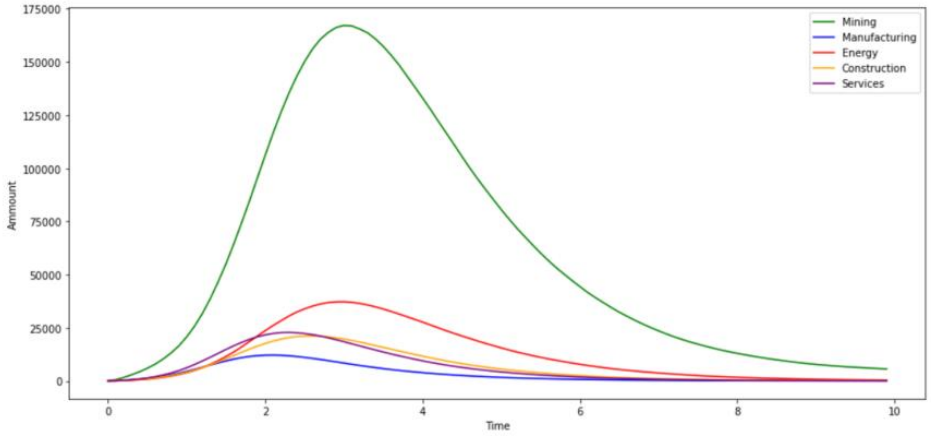
Matrice pour les poids d'adjacence du réseau (d'après les données de HILLAIRET et al., 2021).

Secteur	a	b	Espérance	Variance
Mining	200 000,00	0,5	100 000,00	50 000,00
Manufacturing	10 000,00	0,5	5 000,00	2 500,00
Energy	40 000,00	0,5	20 000,00	10 000,00
Construction	20 000,00	0,5	10 000,00	5 000,00
Services	20 000,00	0,5	10 000,00	5 000,00

$G \sim \mathcal{G}(a, b)$ Paramètres pour les lois générant les pertes par secteurs.

- Modélisation des pertes à l'aide d'une loi Gamma de paramètres a et b
- L'espérance est égale à $a \times b$
- La variance est égale à $a \times b^2$





(a) Nombre d'infectés par secteur au cours du temps. (b) Perte instantanée par secteur au cours du temps.

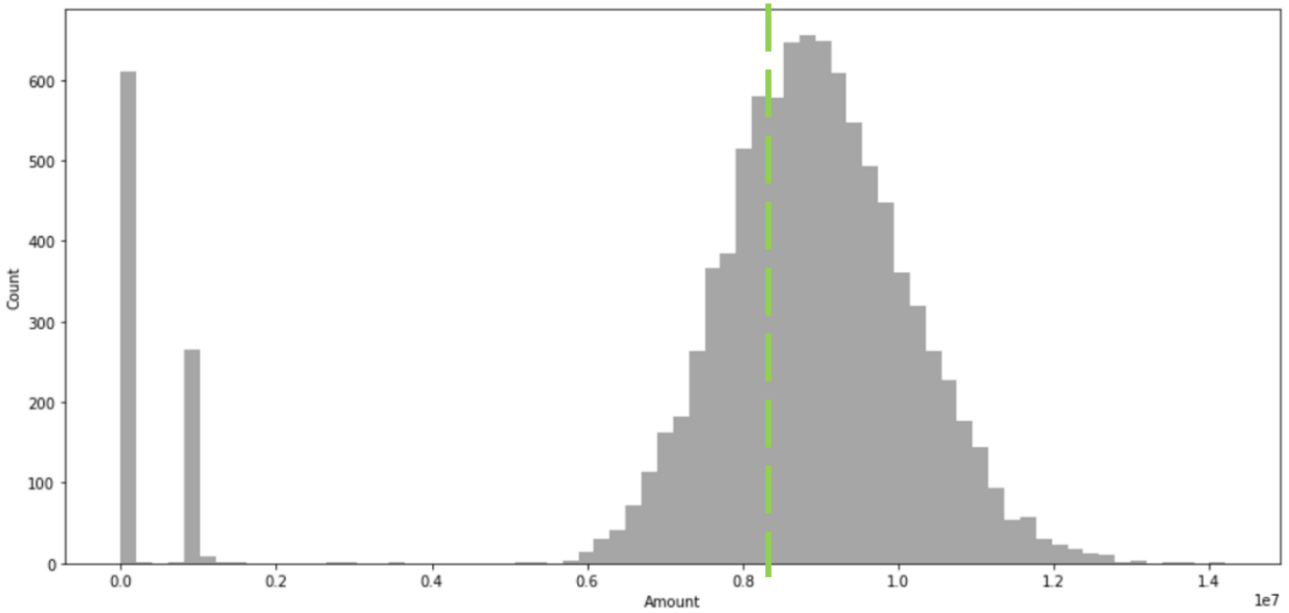
Ordre d'arrivée des pics d'infections

1. Manufacturing
2. Services
3. Construction
4. Energy
5. Mining

Remarques

- Le secteur Mining a le pic d'infection le plus faible mais le plus élevé en coûts
- La figure (a) donne l'évolution du nombre d'infectés au cours du temps
- Les pics surviennent entre 2 et 3 jours après le début de la diffusion et prennent des valeurs entre 50 et 75 infectés

8 204 785 €



Densité des pertes cumulées 10 jours après le début de l'infection.

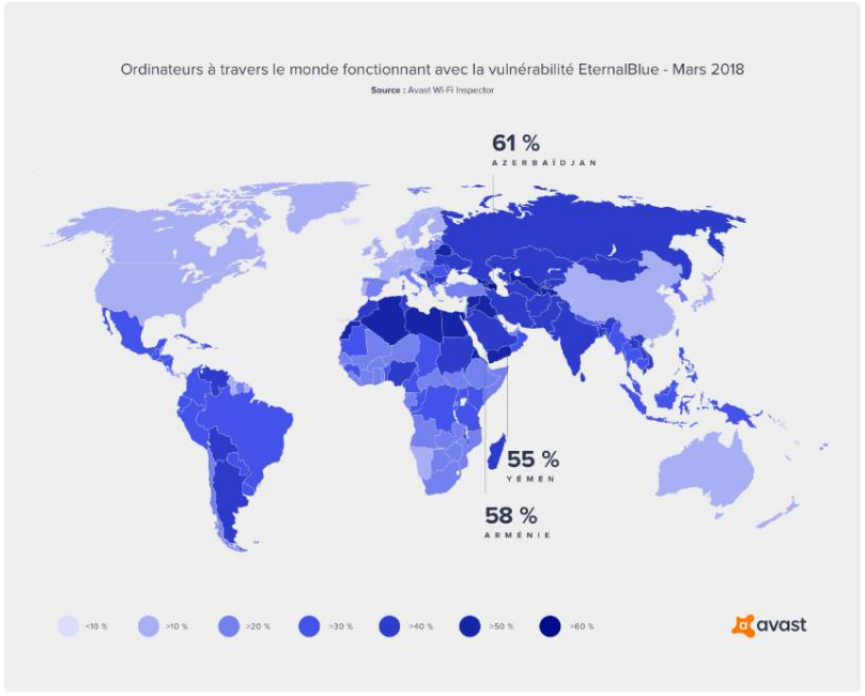
SOMMAIRE

4 Des mesures à prendre

A Augmenter le taux de rétablissement

B Restructurer la répartition des secteurs

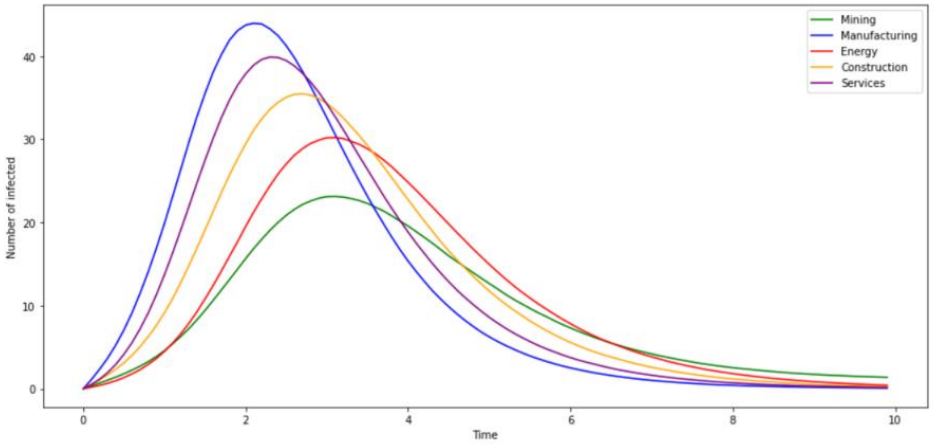
A – Augmenter le taux de rétablissement

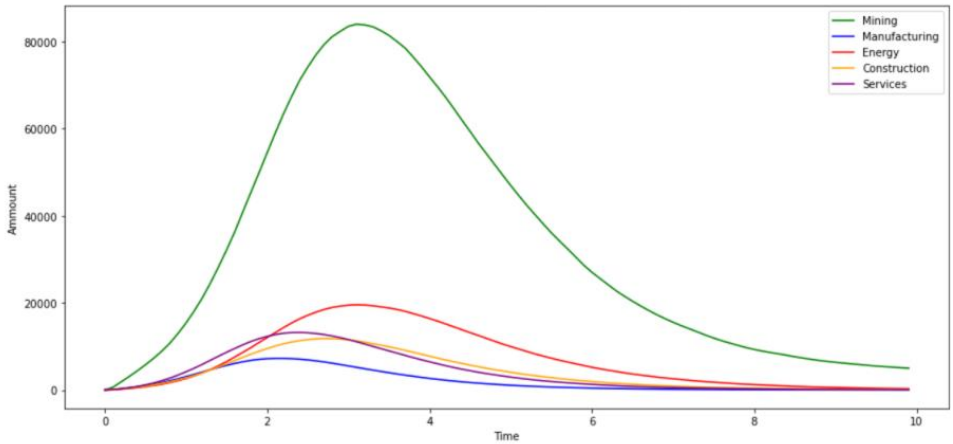


- EternalBlue était exploité par les ransomwares Wannacry et NotPetya.
- EternalBlue est un élément de programme développé par l'Agence de Sécurité Nationale américaine (NSA en anglais) qui exploite une faille de sécurité informatique présente dans le protocole SBMv1 (première version du protocole SMB).
- Le protocole SMB permet aux utilisateurs Windows, de partager des ressources sur des réseaux locaux.

A – Augmenter le taux de rétablissement

$$\gamma = 1,5$$





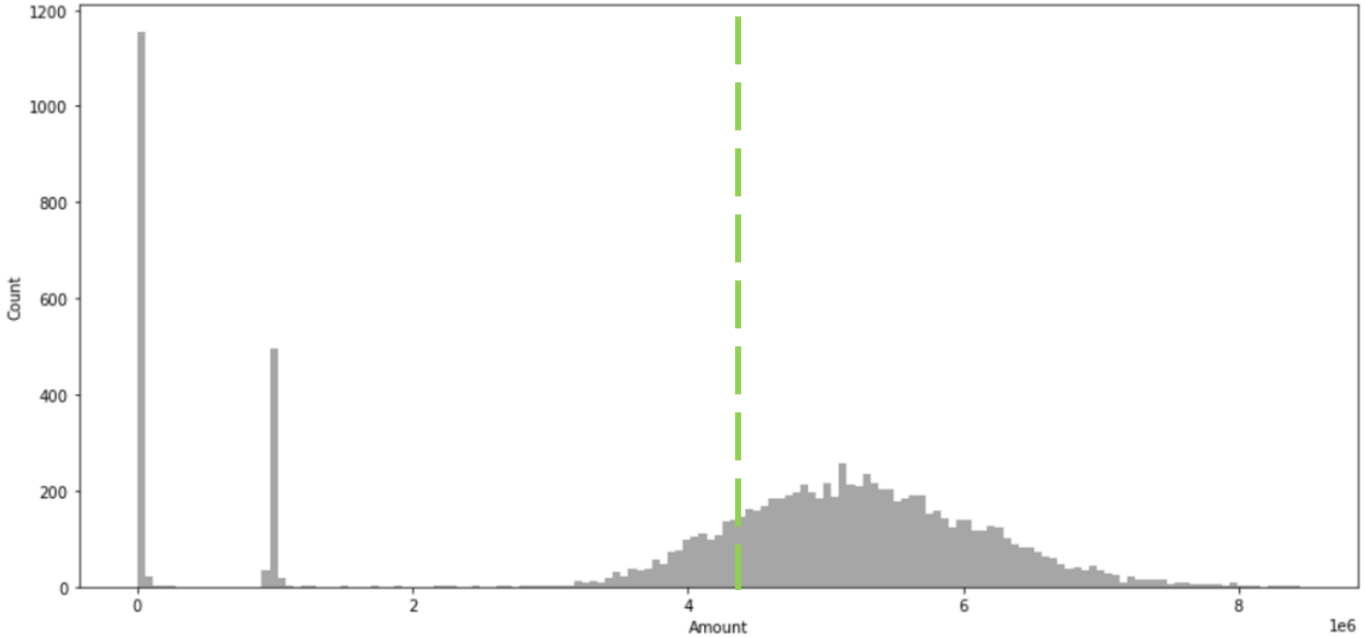
(a) Nombre d'infectés par secteur au cours du temps. (b) Perte instantanée par secteur au cours du temps.

Remarques

- Le temps de rétablissement est d'environ une demi-journée
- L'ordre d'arrivée des pics d'infection reste le même que précédemment
- Le secteur Mining conserve de nouveau le pic d'infection le plus faible mais également le plus élevé en coûts
- Les pics d'infection surviennent de nouveau entre 2 et 3 jours mais les valeurs prises sont plus faibles, entre 23 et 43 infectés.

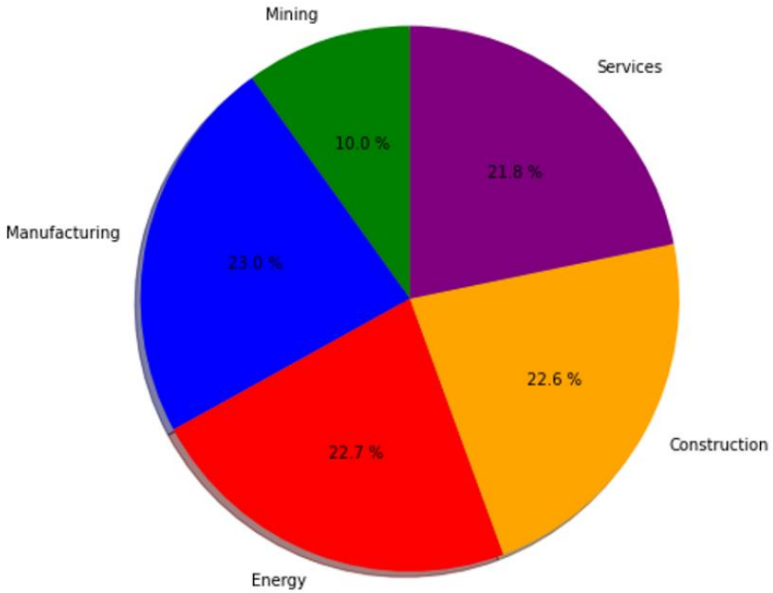
A – Augmenter le taux de rétablissement

4 400 217 €



Densité des pertes cumulées 10 jours après le début de l'infection.

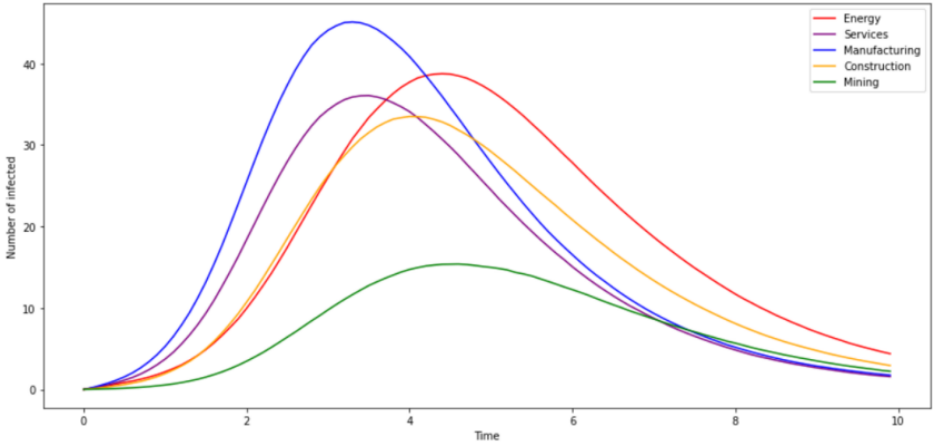
B – Restructurer la répartition du portefeuille



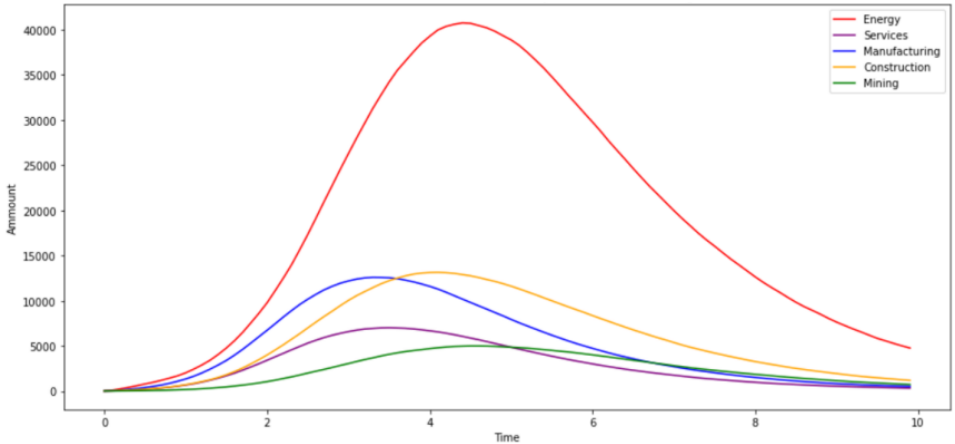
Répartition des assurés selon les différents secteurs au sein du nouveau portefeuille.

B – Restructurer la répartition du portefeuille

$\gamma = 1$



(a) Nombre d'infectés par secteur au cours du temps.



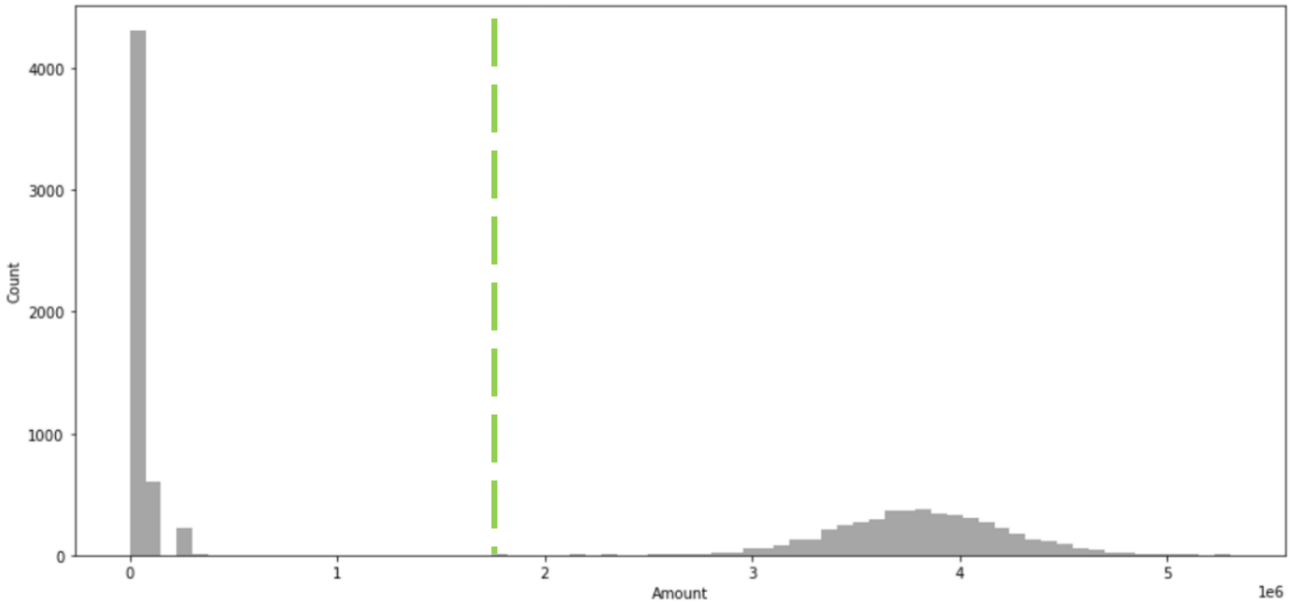
(b) Perte instantanée par secteur au cours du temps.

Remarques

- Le temps de rétablissement est d'environ une journée
- L'ordre d'arrivée des pics est différent que dans les deux scénarios précédents
- Les pics d'infection surviennent entre 3 et 4,5 jours avec des valeurs entre 15 et 45 infectés
- Le secteur le plus cher à indemniser est le secteur Energy tandis que le moins cher est le secteur Mining

B – Restructurer la répartition du portefeuille

1 872 643 €



Densité des pertes cumulées 10 jours après le début de l'infection.

RÉCAPITULATIF

Simulation	Description	Perte moyenne	Commentaire
Référence	Equi-répartition des 1000 assurés dans les 5 secteurs, Figure (3.11). Taux de contagion $\beta = 0.01$. Taux de rétablissement $\gamma = 1$.	8 204 785€	Importante distribution des pertes concentrées autour des 9M€, Figure(3.20).
Taux de rétablissement	Equi-répartition des 1000 assurés dans les 5 secteurs, Figure (3.11). Taux de contagion $\beta = 0.01$. Taux de rétablissement $\gamma = 1.5$.	4 400 217€	Faible distribution autour de 5M€, Figure(3.22). Nombre important de pertes autour de 0.
Restructuration	Distribution des 1000 assurés dans les 5 secteurs, Figure (3.23). Taux de contagion $\beta = 0.01$. Taux de rétablissement $\gamma = 1$.	1 872 643 €	Très faible distribution autour de 3 M€, Figure(3.25). Nombre très important de pertes autour de 0. Double effet généré par la restructuration.

LIMITES DE MODÉLISATION

- **La matrice d'adjacence :** les échanges de valeur ajoutée sont supposés refléter les flux d'informations informatiques entre assurés.

- **La propagation du virus :** il est supposé que le virus se propage qu'au sein du portefeuille que l'on a considéré.

- **Les taux de contagion et de rétablissement :** les taux sont fixés arbitrairement mais peuvent être calibrés de sorte à répliquer des évènements historiques tels que Wannacry.

AUTRES RÉSULTATS

- **Etude de sensibilité I :** illustrer l'influence des paramètres de contagion et de rétablissement sur un graphe homogène.

- **Etude de sensibilité II :** illustrer l'influence du réseau sur la diffusion du virus au sein de la population en reprenant les graphes présentés dans Fahrenwaldt et al., 2018.

- **Etude de sensibilité III :** illustrer l'influence de la condition initiale sur la diffusion du virus dans un contexte cyber en définissant trois scénarios d'infections initiales plausibles, « fournisseur internet, serveur isolé, entreprise moyenne ».

IMPACT DE LA CONDITION INITIALE

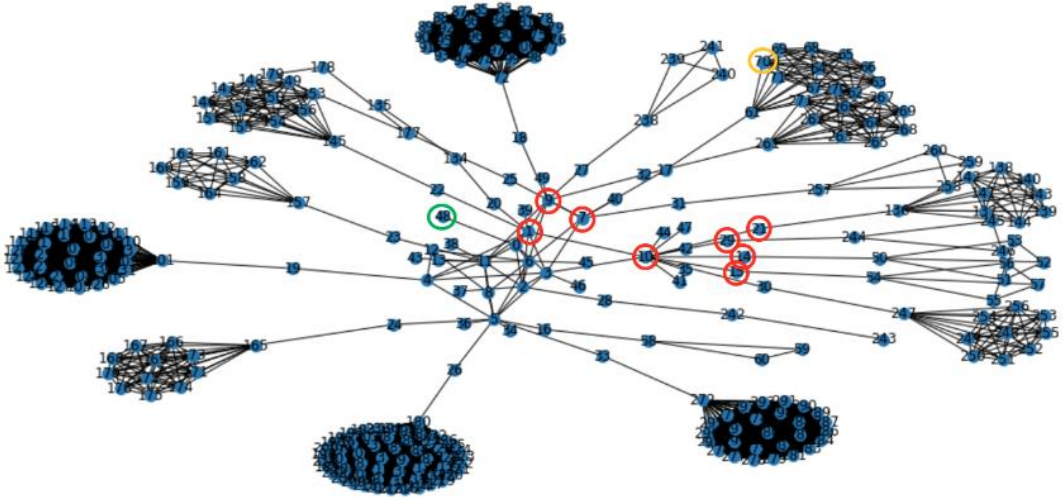
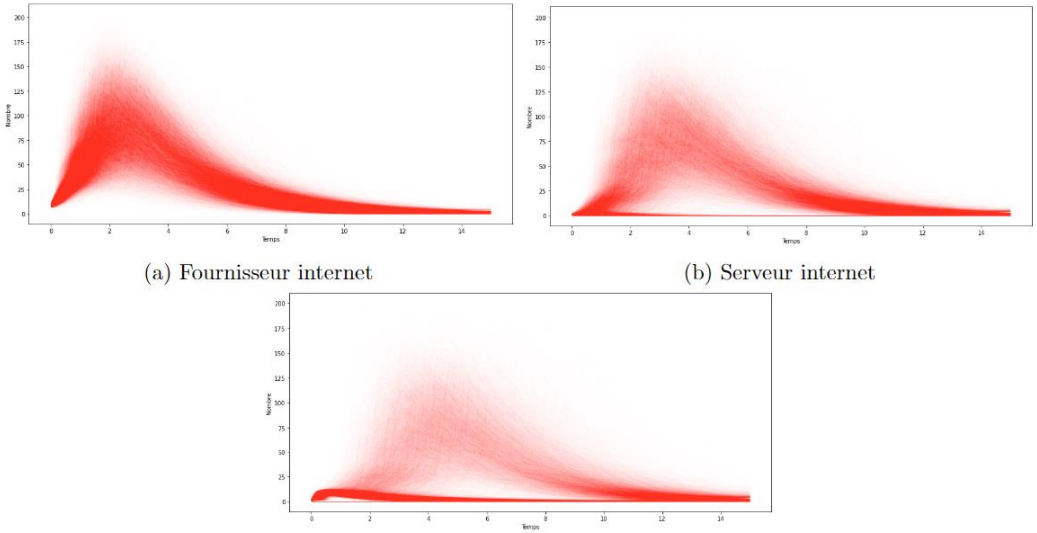


FIGURE 2.26 : Entreprises reliées à internet avec en cercles, les nœuds correspondant aux différentes conditions initiales.

IMPACT DE LA CONDITION INITIALE



(a) Fournisseur internet

(b) Serveur internet

(c) Compagnie moyenne

FIGURE 2.27 : Trajectoires simulées pour le nombre d'infectés au cours du temps pour les différentes initialisations.

OUVERTURES DE MODÉLISATION

- **La structure de réseau :** application à la chaine d'approvisionnement // modélisations des réseaux à partir de données réelles.

- **La propagation du virus :** considérer un plus grand nombre d'assurés // inclure une probabilité d'infection provenant de l'extérieur du réseau.

- **Les taux de contagion et de rétablissement :** rechercher des proxys pour faciliter la simulation et accélérer la calibration du modèle.

- **Le modèle compartimental :** ajout d'un facteur de prévention et/ou d'hygiène cyber // utiliser plus de compartiments pour la diffusion du virus.

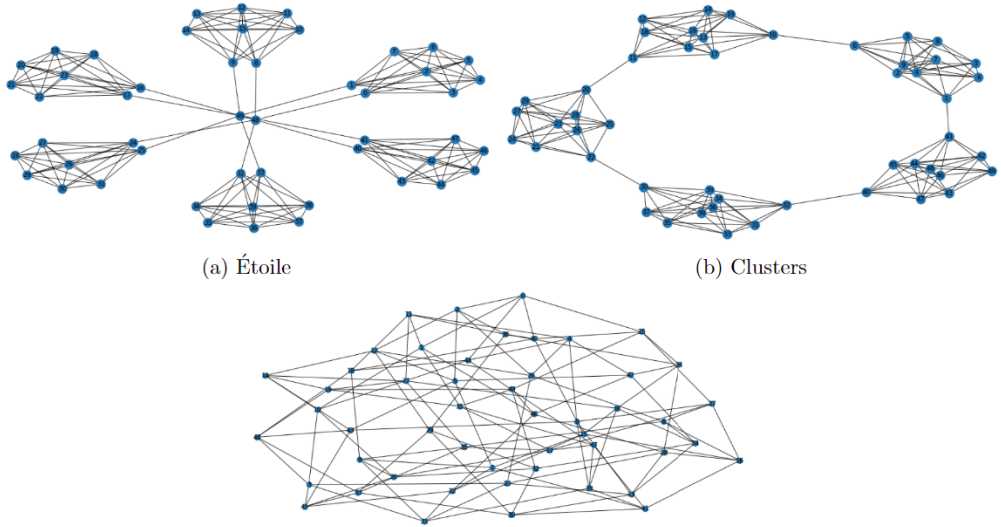
MERCI DE VOTRE ATTENTION

Thomas Peyrat

Le 5 octobre 2023

4, rue Chauveau-Lagarde – 75008 Paris – tél. 01 44 51 72 72
www.institutdesactuaires.com

IMPACT DE LA STRUCTURE DU RÉSEAU



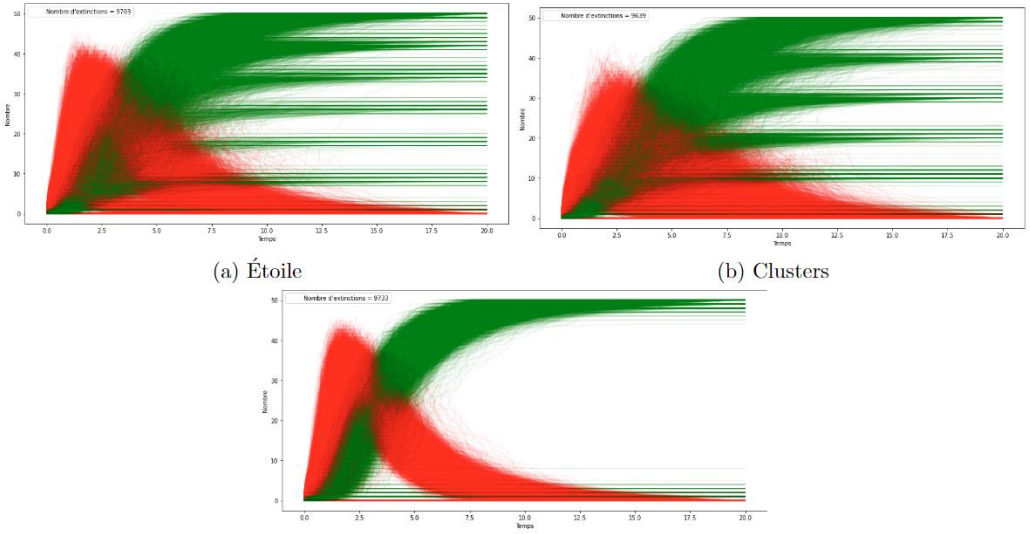
(a) Étoile

(b) Clusters

(c) Degré 5

FIGURE 2.23 : Différentes topologies de réseaux.

IMPACT DE LA STRUCTURE DU RÉSEAU



(a) Étoile

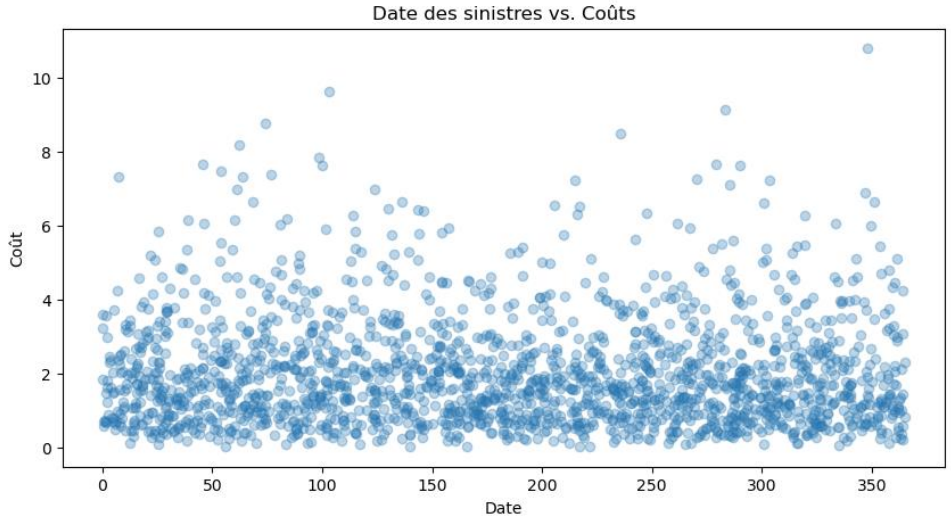
(b) Clusters

(c) Degré 5

FIGURE 2.24 : Simulations (10 000) pour le nombre d'infectés (en rouge) et de rétablis (en vert) dans le modèle SIR pour les réseaux de la figure(2.23). Plus les couleurs ressortent, plus le nombre de simulations à suivre cette trajectoire sont importantes.

LES DONNÉES USUELLES

Observations du montant des sinistres



Répartition des sinistres dans le temps

UN MODÈLE SIMPLE

Nombre de sinistre jusqu'au temps t

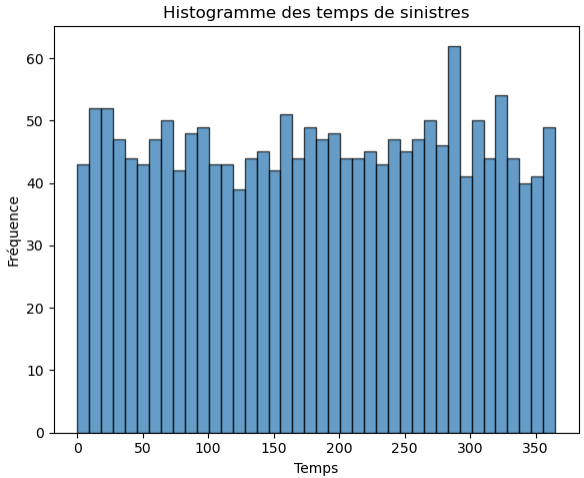
Montant total à indemniser jusqu'au temps t

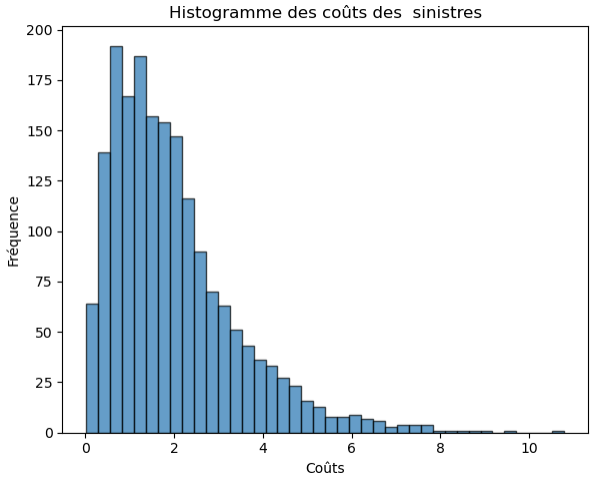
$$C_t = \sum_{i=1}^{N_t} X_i$$

Montant du *i-eme* sinistre

$$C_{365} = \sum_{i=1}^{N_{365}} X_i$$

UN MODÈLE SIMPLE





UN MODÈLE SIMPLE

$$\mathbb{E}[C_{365}] = \mathbb{E}[N_{365}] \times \mathbb{E}[X]$$

« La moyenne » du total annuel à indemniser

« La moyenne » du nombre de sinistres par an

« La moyenne » du coût d'un sinistre