Modélisation de la fréquence du risque cyber à l'aide des processus de Hawkes

Yousra Zirnheld, Milliman R&D - CREST Ensae

Sous la direction de :

Alexandre Boumezoued, Milliman R&D
Caroline Hillairet, CREST Ensae

Congrès des actuaires
17 juin 2025

Milliman

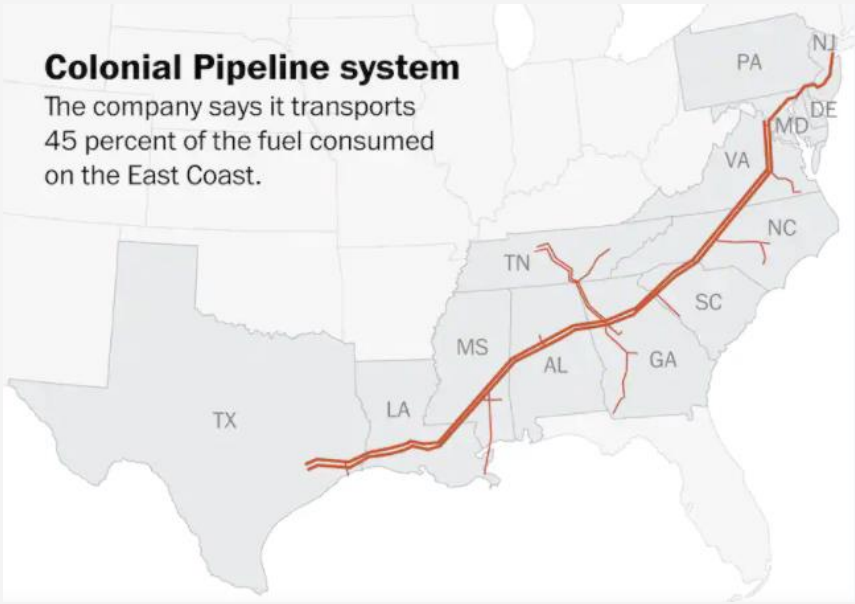
CREST
CENTER FOR RESEARCH IN ECONOMICS AND STATISTICS

Risque cyber

Quelques exemples d'incidents numériques notables

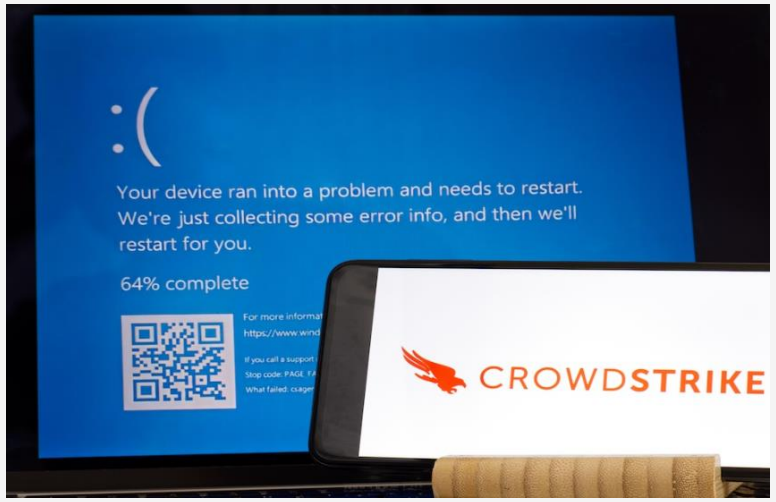
Wannacry/NotPetya (2017)

Attaque informatique



Colonial Pipeline (2021)

Attaque informatique



Crowdstrike (2024)

Incident informatique

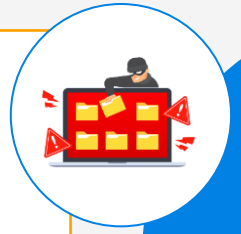
Risque cyber

Et l'assurance dans tout ça ?

- Plusieurs types de couvertures sont proposées en lien avec les dommages occasionnés : **les dommages directs subis par l'assuré**, **ceux pour lesquels il peut être tenu responsable,** ainsi que **les frais additionnels engendrés par l'incident .**

First Party

- **Perte d'exploitation**
- **Vol de propriété intellectuelle**
- **Dommages aux biens matériels**
- **Atteinte à la réputation**



Exemples de garanties proposées

Third Party

- **Responsabilité en cas de fuites de données sensibles**
- **Responsabilité en cas de défaillance des services informatiques**
- **Responsabilité des dirigeants et administrateurs**

Frais supplémentaires

- **Inspection des systèmes IT et mises à jours globales**
- **Frais judiciaires**

- Mais à la différence d'autres risques assurables, **le risque cyber est systémique**, **en constante évolution, multiforme et souvent sous-déclaré** et souffre **d'un manque de données historiques**, ce qui complique fortement son évaluation.
- Pour y répondre, des **outils mathématiques avancés** sont nécessaires afin de **modéliser dynamiquement sa fréquence et sa sévérité**, et ainsi permettre **une tarification et une gestion du risque** plus fiables.

Objectifs de la thèse

Proposer des outils mathématiques pour modéliser la fréquence des attaques informatiques

Modélisation de la fréquence à l'aide des processus de Hawkes

1 🎯 Modéliser l'impact des vulnérabilités informatiques sur les attaques

💡 Les attaques informatiques peuvent survenir de l'exploitation des vulnérabilités informatiques

🛠️ *Processus de Hawkes avec excitation externe*

2 🎯 Modéliser l'hétérogénéité dans la contagiosité

💡 Les attaques informatiques ne se propagent pas de la même manière

🛠️ *Processus de Hawkes avec des marques aléatoires, Algorithmes CART avec des critères de split adaptés*

3 🎯 Quantifier l'impact des mesures de réaction

💡 Les conséquences des attaques peuvent être limitées grâce à une réaction rapide et adaptée

🛠️ *Processus de Hawkes en deux phases*

Modélisation de la fréquence des cyber-attaques

Processus de Hawkes

Le **nombre de sinistres** à l'instant **t (Composante fréquence)**

Perte totale d'un portefeuille cyber

$$L(t) := \sum_{i=1}^{N_t} Y_i$$

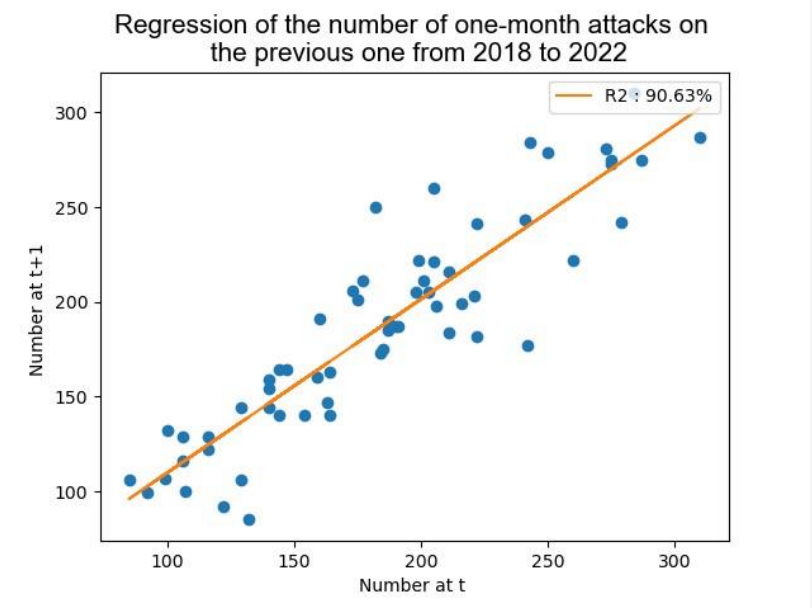
Le coût du $i^{ème}$ sinistre (Composante sévérité)

- Un **processus de Hawkes** est un processus de comptage $N(t) = \sum_{n\geq 1} 1_{T_n \leq t}$ avec une intensité de la forme:

$$\lambda_t = \lambda_0 + \sum_{T_i<t} \phi(t - T_i)$$

Intensité de base — Noyau d'excitation

- La somme $\sum_{T_n<t} \phi(t - T_n)$ représente **l'impact des évènements passés** et capture la propriété d'**auto-excitation**. Ces processus modélisent **l'arrivée d'évènements en cascade** et des **changements de régime.**
- Ils sont **paramétriques** et **tractables**



Modélisation de la fréquence des attaques informatiques

Processus de Hawkes avec excitation externe

1

🎯 Modéliser l'impact des vulnérabilités informatiques sur les attaques

💡 Les attaques informatiques peuvent survenir de l'exploitation des vulnérabilités informatiques

🛠️ *Processus de Hawkes avec excitation externe :*

$$\lambda_t = \lambda_0 + \sum_{\overline{T_k}<t} \overline{\phi}(t-\overline{T_k}) + \sum_{T_i<t} \phi(t-T_i)$$

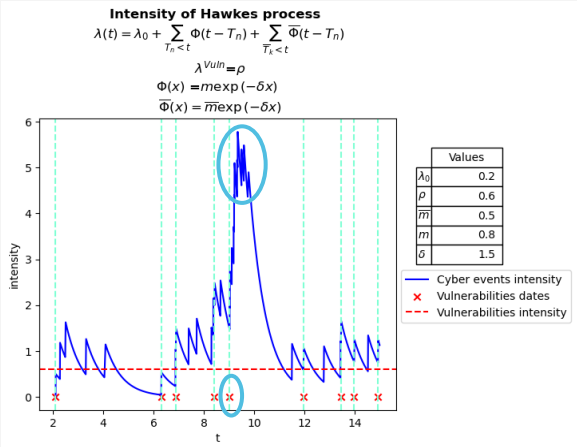
Modélisation de la fréquence à l'aide des processus de Hawkes

2

🎯 Modéliser l'hétérogénéité dans la contagiosité

💡 Les attaques informatiques ne se propagent pas de la même manière

🛠️ *Processus de Hawkes avec des marques aléatoires, Algorithmes CART avec des critères de split adaptés*



3

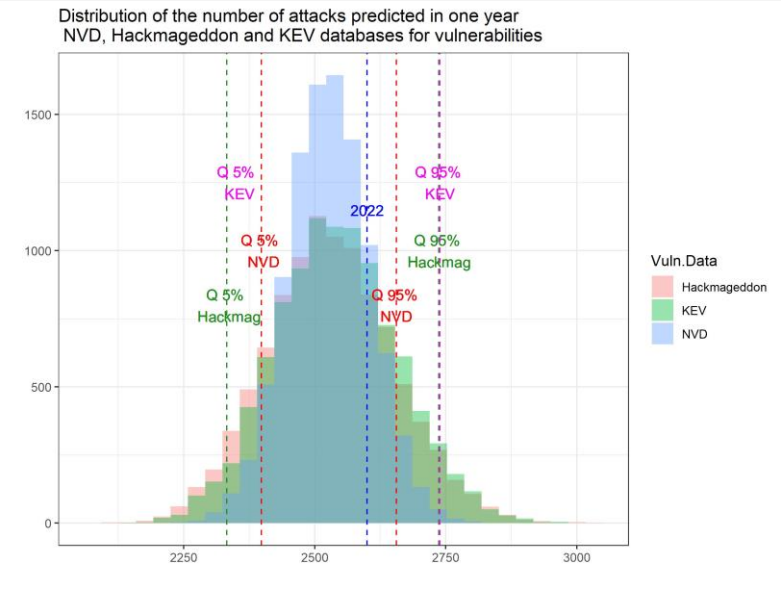
🎯 Quantifier l'impact des mesures de réaction

💡 Les conséquences des attaques peuvent être limitées grâce à une réaction rapide et adaptée

🛠️ Processus de Hawkes en deux phases

Quelques résultats de calibrage

Model	Vuln. database	λ_0	ρ	$\overline{m}$	m	δ	$\|\|\phi\|\|$
No external events	-	2.7031	-	-	0.9182	1.5047	0.61
	95% C.I	[2.4863,2.9199]	-	-	[0.8608, 0.9756]	[1.1723, 1.8371]	-
With external events	Hackmageddon	2.7081	0.3636	0.5941	0.8891	1.5080	0.58
	95% C.I	[2.4873,2.9289]	[0.3180, 0.4092]	[0.3484, 0.8398]	[0.6909, 1.0873]	[1.1649, 1.8511]	-
With external events	KEV	2.6964	0.5057	0.9774	0.8529	1.5061	0.56
	95% C.I	[2.4229, 2.9699]	[0.4527, 0.5587]	[0.4388, 1.2282]	[0.6734, 1.1048]	[1.1921, 1.8239]	-
With external events	NVD	2.4195	48.849	0.077413	0.67139	1.8697	0.36
	95% C.I	[2.1573,2.6817]	[48.2987,49.1993]	[0.01211,0.1427]	[0.4985,0.8442]	[1.3998,2.3396]	-



- Le calibrage a été effectué à partir **des bases de données** suivantes : **Hackmageddon** (attaques), **NVD** et **KEV** (vulnérabilités informatiques).
- $\| \phi \|$ (le degré d'endogénéité du système) représente **le nombre moyen d'attaques** qu'une attaque va engendrer.
- $\| \phi \|$ est presque **réduit de moitié entre le modèle sans excitation externe** et le modèle avec excitation externe provenant de la base de données NVD.

Modélisation de la fréquence des attaques

Processus de Hawkes avec excitation externe et marques aléatoires

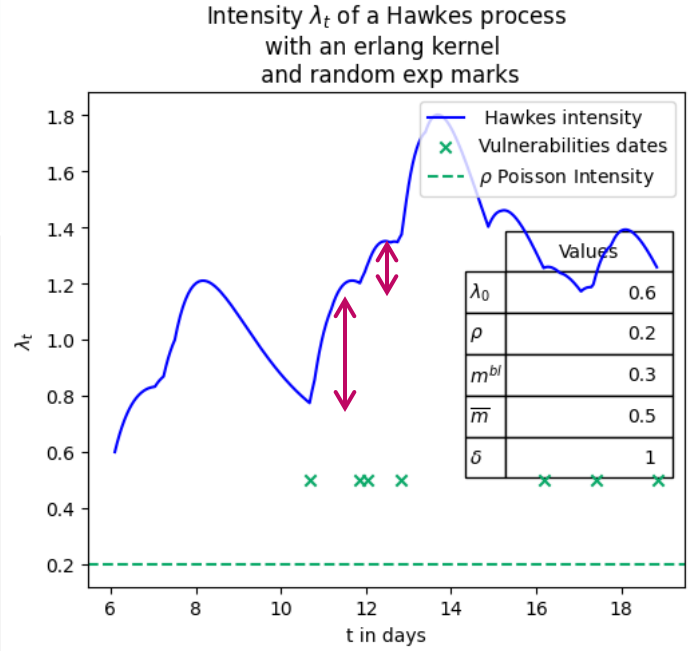
Modélisation de la fréquence à l'aide des processus de Hawkes

2 Modéliser l'hétérogénéité dans la contagiosité

Les attaques informatiques ne se propagent pas de la même manière

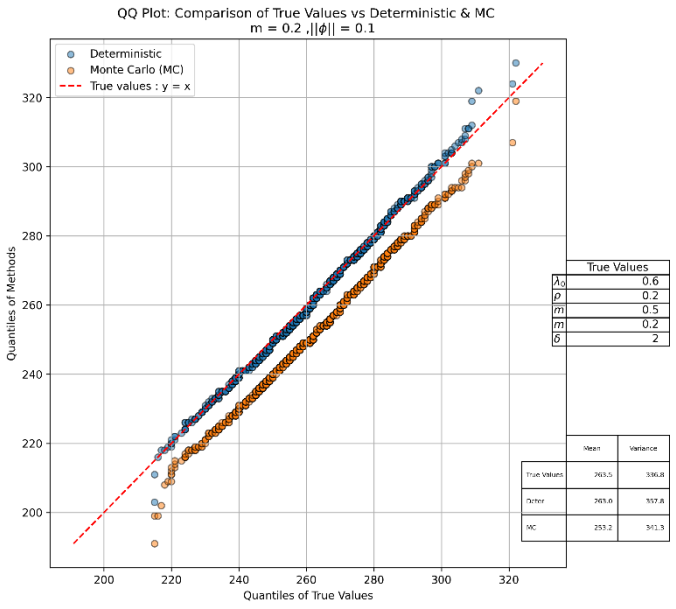
Processus de Hawkes avec des marques aléatoires

$$\lambda_t = \lambda_0 + \sum_{\overline{T_k}<t} \overline{\phi}\left(t - \overline{T_k}, \overline{Y_k}\right) + \sum_{T_i<t} \phi(t - T_i, Y_i)$$

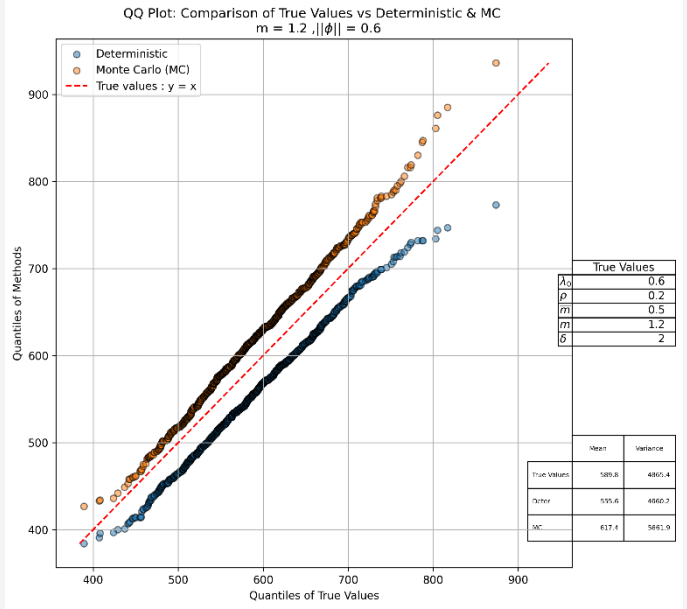


Développement de méthodes de calibrage adaptées

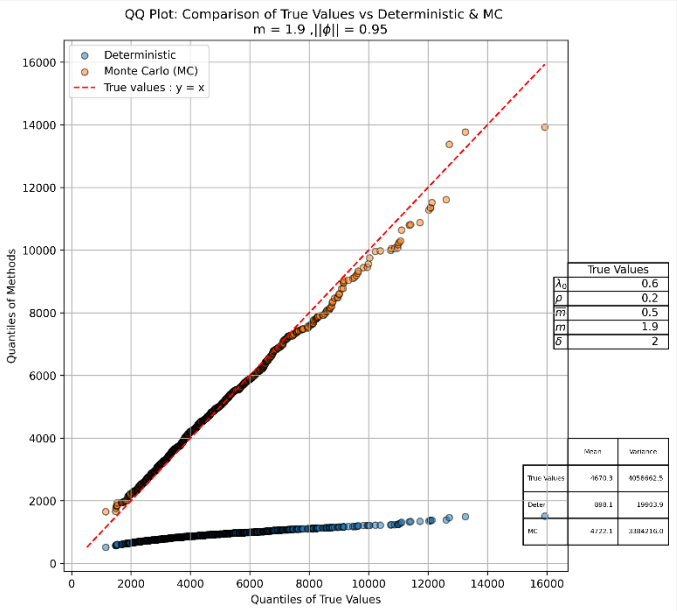
Quelques résultats sur les distributions prédites



Petite variance



Variance moyenne



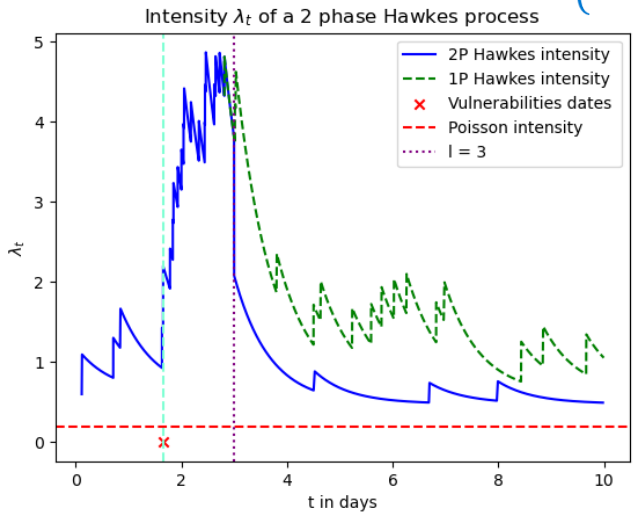
Variance élevée

- **Le choix de la méthode de calibrage** dépend de la **contagiosité des attaques considérées**.

Modélisation de la fréquence des attaques

Processus de Hawkes en deux phases

$$\lambda_t = \begin{cases} \underbrace{\lambda_0}_{\text{Baseline intensity}} + \underbrace{\sum_{\overline{T_k}<t} \overline{Y_k}\, e^{-\delta(t-\overline{T_k})}}_{\text{External excitation : cyber vulnerabilities}} + \underbrace{\sum_{T_i<t} Y_i^{bl}\, e^{-\delta(t-T_i)}}_{\text{Self excitation : cyber attacks}} & \text{if } t \leq \underbrace{\ell}_{\text{Reaction time}} \\ \underbrace{\alpha_0}_{\text{Reaction parameter}}\lambda_0 + \underbrace{\alpha_1}_{\text{Reaction parameter}}(\lambda_{\ell^-} - \lambda_0) & \text{if } t = \ell \\ \alpha_0\lambda_0 + \alpha_1(\lambda_{\ell^-} - \lambda_0)e^{-\delta(t-\ell)} + \sum_{\ell<T_i<t} Y_i^{al}\, e^{-\delta(t-T_i)} & \text{if } t > \ell \end{cases}$$



3

🎯 Quantifier l'impact des mesures de réaction

💡 **Les conséquences des attaques peuvent être limitées grâce à une réaction rapide et adaptée**

🛠️ Processus de Hawkes en deux phases

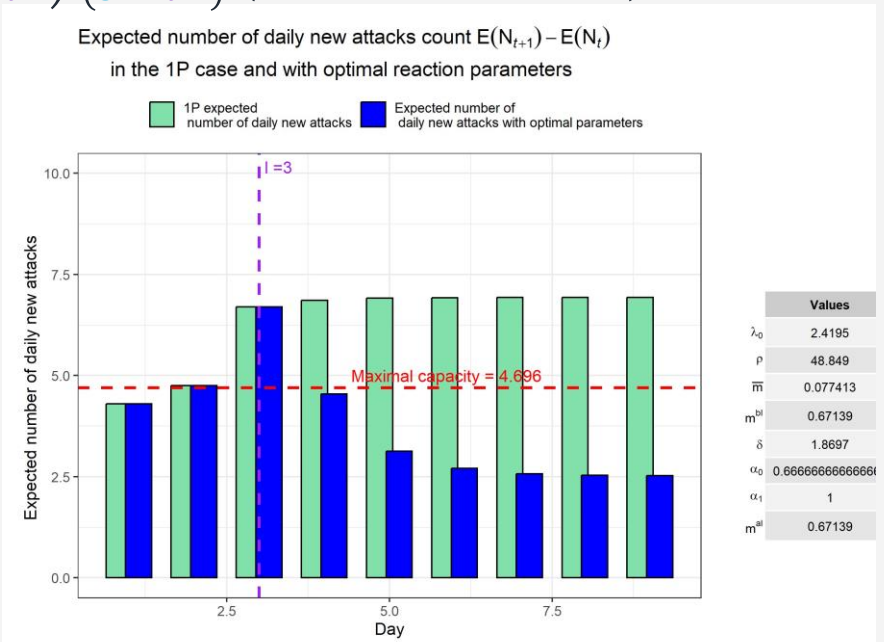
Mesures de réaction à l'aide la deuxième phase

Sélection de paramètres optimaux

For t> ℓ > s :

$$\mathbb{E}[N_t|\mathcal{F}_s]=\begin{cases}\mathbb{E}[N_\ell|\mathcal{F}_s]+\frac{\alpha_0\delta\lambda_0}{2}(t-\ell)^2+\lambda_0(\alpha_0-\alpha_1)(t-\ell)+\alpha_1\mathbb{E}[\lambda_{\ell^-}|\mathcal{F}_s](t-\ell) & \text{if } \delta=m^{al}\\ \mathbb{E}[N_\ell|\mathcal{F}_s]+\frac{\alpha_0\delta\lambda_0}{\delta-m^{al}}(t-\ell)+\left((\alpha_0-\alpha_1)\lambda_0+\alpha_1\mathbb{E}[\lambda_{\ell^-}|\mathcal{F}_s]-\frac{\alpha_0\delta\lambda_0}{\delta-m^{al}}\right)\frac{1}{(\delta-m^{al})}\left(1-e^{-(\delta-m^{al})(t-\ell)}\right) & \text{if } \delta\neq m^{al}\end{cases}$$

- **Assureur fictif** avec **une capacité de réaction limitée** à 5 assurés par jour
- Calculer **les paramètres de réponse** adéquats de manière **à ne pas dépasser cette capacité** en moyenne.



Conclusion

- Comprendre le lien entre vulnérabilités et attaques : modélisation via un processus de Hawkes avec excitation externe
- Capturer l'hétérogénéité des dynamiques d'attaque : utilisations de marques aléatoires et des arbres aléatoires CART (non détaillé dans cette présentation)
- Evaluer l'impact des mesures de réaction : intégration d'une phase de réaction dans le modèle pour quantifier ces effets
- Objectif global : fournir des outils mathématiques pour quantifier ce risque