Cyber risk modeling using a two-phase Hawkes Process with external excitation

Yousra Cherkaoui, Milliman R&D - CREST Ensae

Joint work with :

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

Insurance Data Science
June 18th, 2024

Milliman

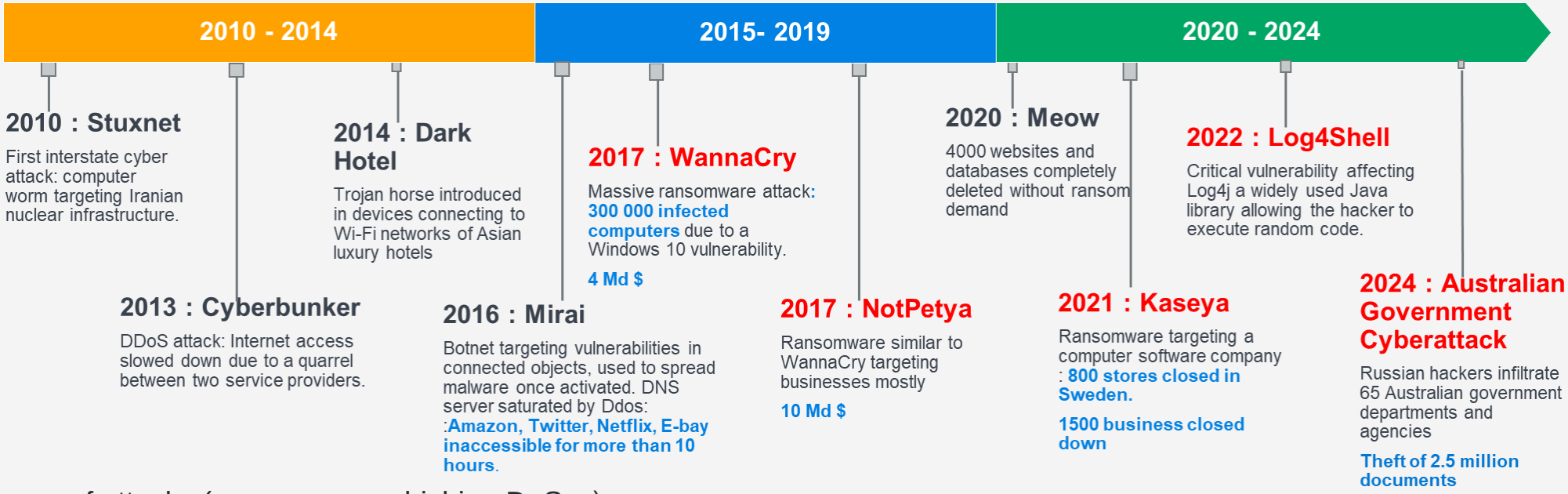
CREST
CENTER FOR RESEARCH IN ECONOMICS AND STATISTICS

Agenda

- Context
- Cyber risk modelling using Hawkes processes with vulnerabilities
- Cyber attacks and vulnerability databases
- Calibration results of the One-Phase Hawkes process
- Response measures using the second phase of the Hawkes process
- Future research questions

Cyber risk

Context



- **Various types** of attacks (ransomware, phishing,DoS…)
- Focus on **contagious** cyber incidents, by taking into account the exploitation of **cyber vulnerabilities** (exogenous excitation)
- Regular publications of **vulnerabilities** that may cause **cyber pandemics :** EternalBlue (Wannacry, NotPetya), Log4Shell etc
- **Quantifying** impact of **protection measures** to **limit the effect of a cyber attack** (patching vulnerabilities for instance)

Cyber risk frequency modeling

Objectives

Frequency modelling using Hawkes processes

1

Grasp internal excitations through Hawkes frequency process

Bessy-Roland, Y., Boumezoued, A., & Hillairet, C. (2021). Multivariate Hawkes process for cyber insurance. Annals of Actuarial Science, 15(1), 14-39.

2

Add external excitation into the modelling : vulnerabilities publication that may trigger cyber attacks

Dassios, A., & Zhao, H. (2011). A dynamic contagion process. Advances in applied probability, 43(3), 814-846.

3

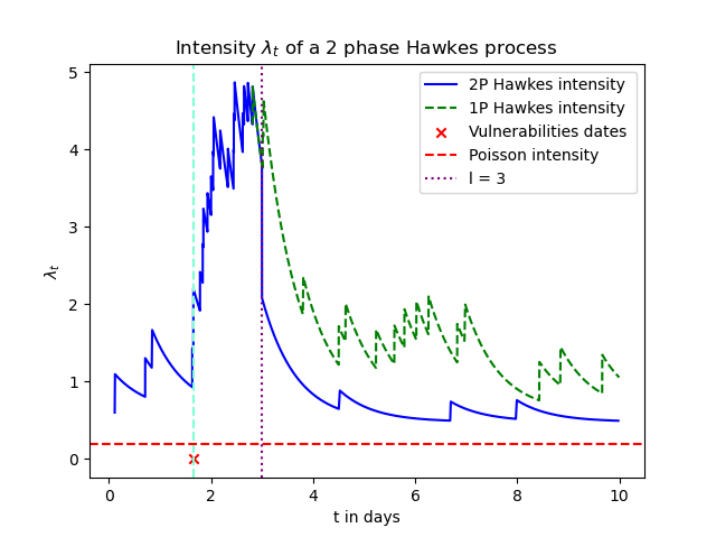
Model the reaction measures using a two-phase Hawkes proces

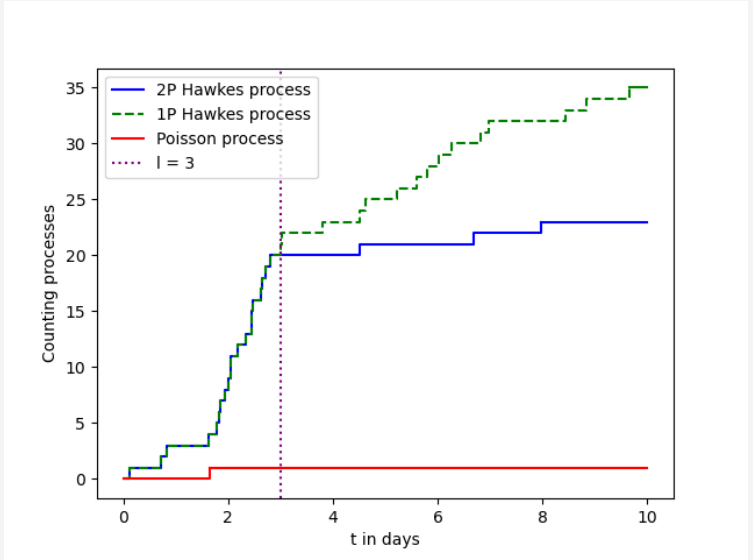
Chen, Z., Dassios, A., Kuan, V., Lim, J. W., Qu, Y., Surya, B., & Zhao, H. (2021). A two-phase dynamic contagion model for COVID-19. Results in Physics, 26, 104264.

Cyber risk modelling

A Two-Phase Hawkes process with external excitation

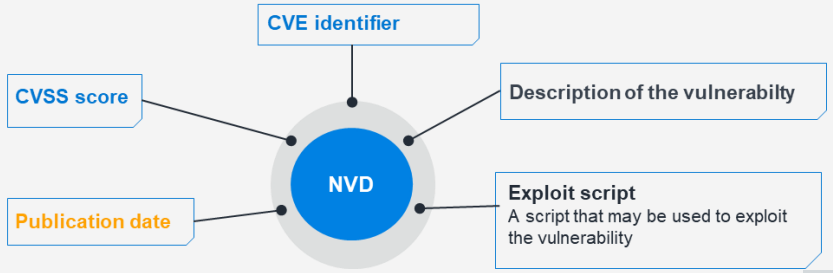
$$\lambda_t = \begin{cases} \underbrace{\lambda_0}_{\text{Baseline intensity}} + \underbrace{\sum_{T_k<t} Y_k\, e^{-\delta(t-T_k)}}_{\text{External excitation : cyber vulnerabilities}} + \underbrace{\sum_{T_i<t} Y_i^{bl}\, e^{-\delta(t-T_i)}}_{\text{Self excitation : cyber attacks}} & \text{if } t \leq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

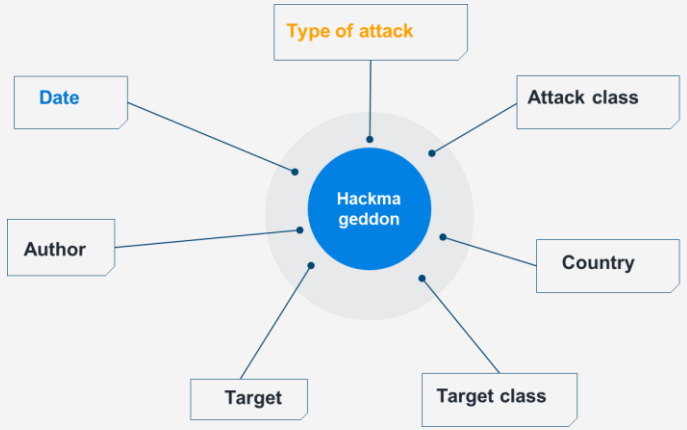




Cyber databases

Hackmageddon and NVD databases



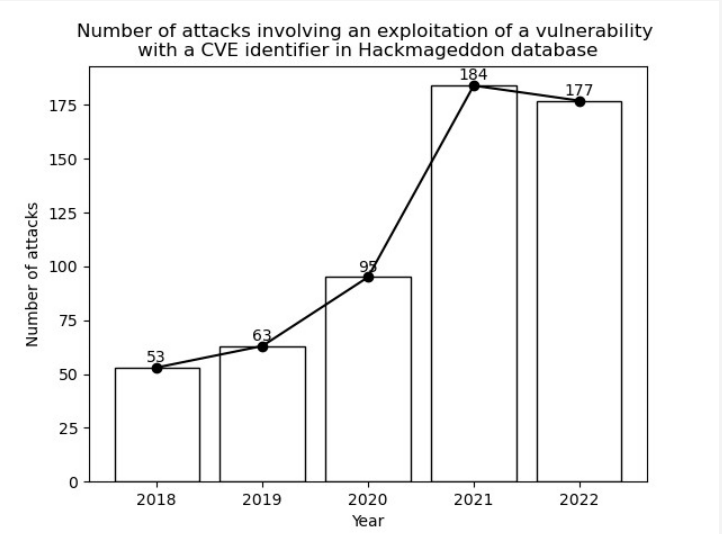


$$\lambda_t = \underbrace{\lambda_0}_{\text{Baseline intensity}} + \underbrace{\sum_{T_k<t} \overline{m}\, e^{-\delta(t-\overline{T_k})}}_{\text{External excitation : cyber vulnerabilities}} + \underbrace{\sum_{T_i<t} m\, e^{-\delta(t-T_i)}}_{\text{Self excitation : cyber attacks}}$$

CVE (Common Vulnerability Exposure) **publication dates**

Cyber attacks dates

Different countries are represented in this database - The US is still the most represented

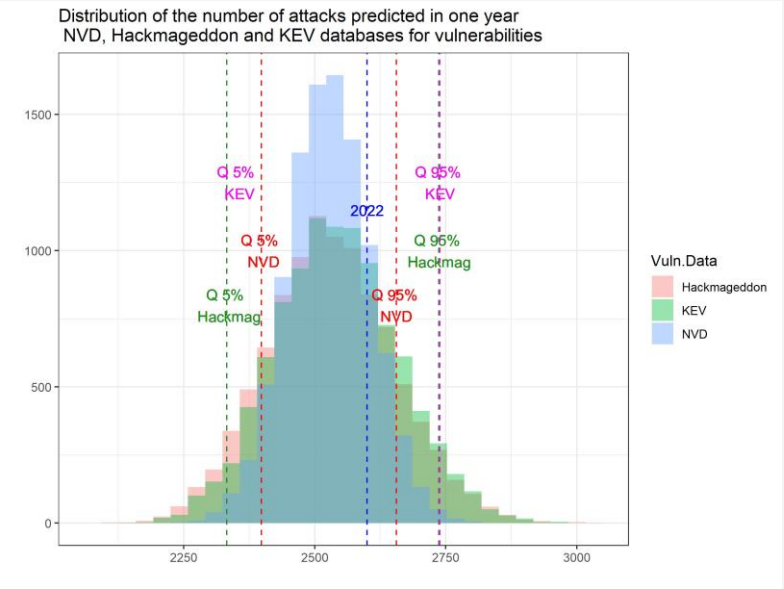


Growing number of attacks involving a **CVE identifier**

Calibration of the one-phase Hawkes process

Calibration results

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]	-



- $\| \phi \|$ (the **endogeneity degree** of the system) represents the **average number** of attacks **an attack** will lead to.
- $\| \phi \|$ is nearly **halved** between the **model with no external excitation** and the model with the **external excitation taken from the NVD database.**
- The distributions seem to **capture the dynamics of cyber attacks in 2022** for the **Hackmageddon** database.
- The **distribution of the number of attacks** with vulnerabilities from the **NVD** database has the **smallest variance**.
- This **decrease in variance** has significant implications in **insurance reserve calculations**, for example.

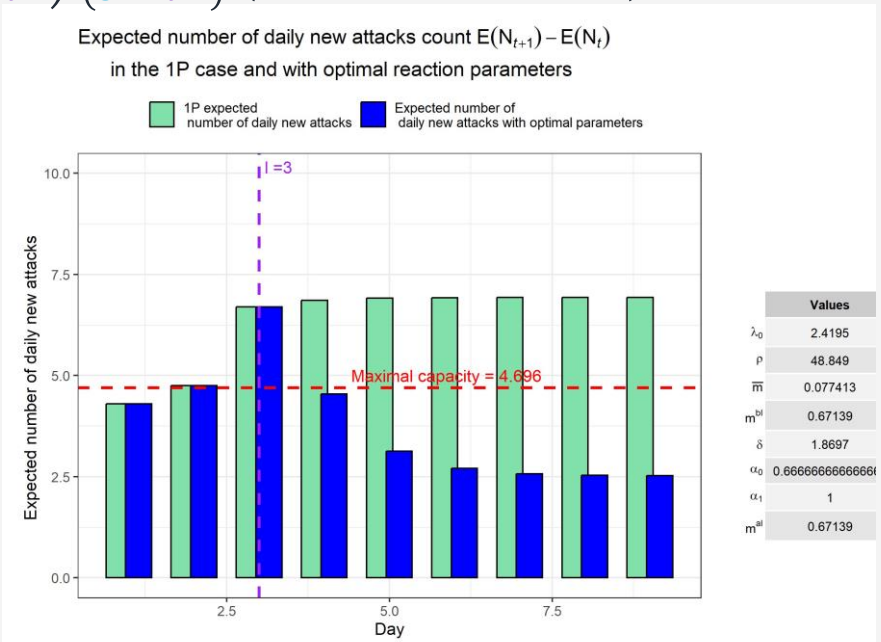
Response measures using the second phase of the process

Parameters selection

For t> ℓ > s :

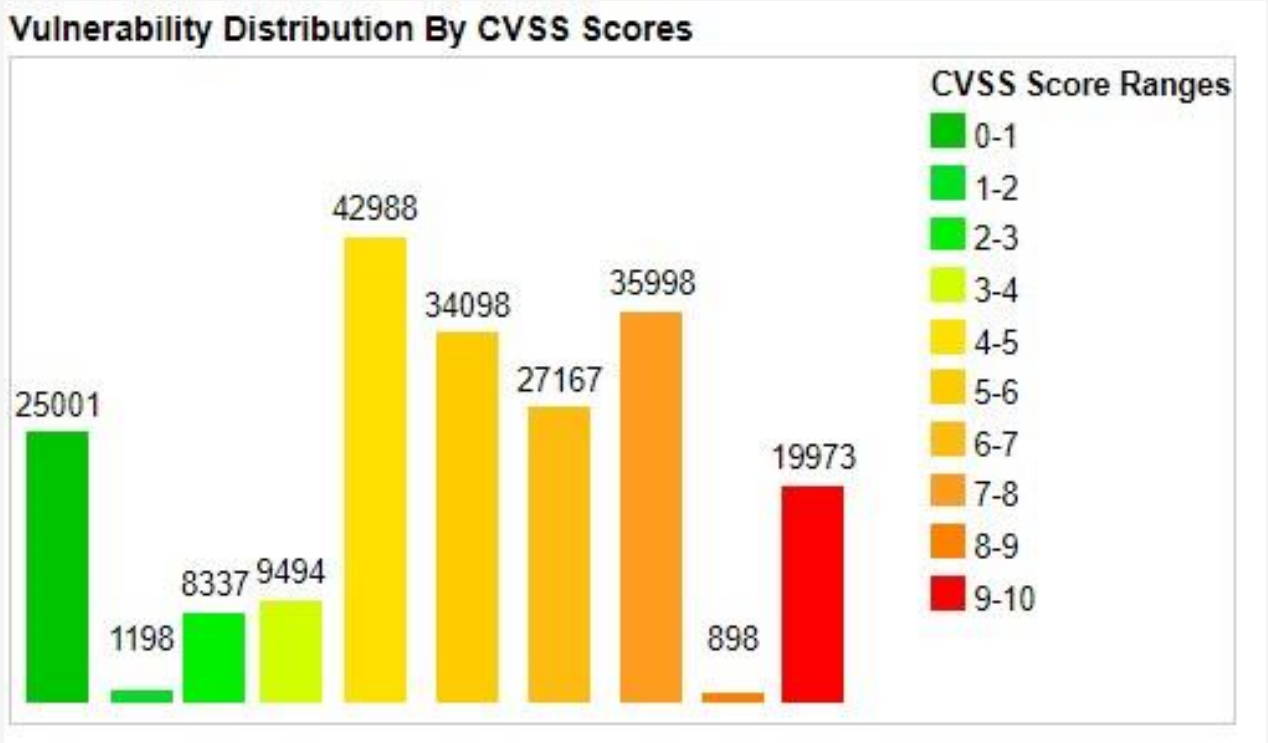
$$\mathbb{E}[N_t|\mathcal{F}_s]=\begin{cases}\mathbb{E}[N_\ell|\mathcal{F}_s]+\frac{\alpha_0\delta\lambda_0}{2}(t-\ell)^2+\lambda_0(\alpha_0-\alpha_1)(t-\ell)+\alpha_1\mathbb{E}[\lambda_{\ell^-}|\mathcal{F}_s](t-\ell) & \text{if } \delta=m^{al}\\ \mathbb{E}[N_\ell|\mathcal{F}_s]+\frac{\alpha_0\delta\lambda_0}{\delta-m^{al}}(t-\ell)+\left((\alpha_0-\alpha_1)\lamb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

- **Fictional insurer** with a **limited reaction capacity** of 5 policyholders each day
- Compute **the adequate response parameters** such that the **response capacity** is **not exceeded on average**



Future research questions

Paper available at :



- Extension to the **delay kernel** and **random marks**
- Develop **statistical classification and regression models** (such as CART trees) whose **classification criterion is based on the excitation of Hawkes processes**