Quantifying Stressed Scenarios of Cyber Loss Processes with Dynamic Dependencies

Caroline Hillairet, ENSAE IP Paris, CREST

Joint works with Y. Cherkaoui and T. Peyrat (CREST)
A. Réveillac (Institut de Mathématiques de Toulouse)

Paris, ECA 2026, 18-19 June 2026

Need of dynamic models for cyber risk

- Cyber risk is new and constantly evolving : Emerging risk that remains emerging because it is constantly changing (very difficult to predict, need to react very quickly).
  - Fast development of new numerical tools (Gen IA)
  - Fast adaptation of the attackers (in case of malicious cyber).
- (Generative) AI
  - amplifies cyber risk,
  - increases systemic risk (Interconnections and AI supply chains)
- Need for Dynamic models to take into account
  - Stochastic changes in the intensity of arrival of events
  - Strong and complex dependencies (between events, policyholders, other risks) especially in extreme scenarios.
- Continuous time model well suited for a high-frequency monitoring of the risk.

ENSAE
IP PARIS

Cumulative Loss process

$$L_t := \sum_{i=1}^{N_t} C_i, \quad t \in [0, T],$$

- Frequency: Claims arrival modeled by a counting process $N := (N_t)_{t\in[0,T]}$, jumping at time $(\tau_i)_{i\in\mathbb{N}^*}$,
- Severity: claims sizes $(C_i)_{i\in\mathbb{N}^*}$

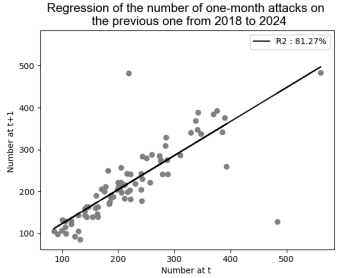
Classical **Cramer-Lundberg** model

- N is a Poisson process (inter-arrivals $(\tau_i - \tau_{i-1})$ are iid)
- N is independent of the claims sizes (C_i),
- (C_i) iid random variables.

CL $\Rightarrow$ Tractable computations due to the independence assumptions $\cdots$ but they are not satisfied for cyber risk (and systemic risk).

Autocorrelation of the number of cyber-events

- **Hackmageddon database**, maintained by Paulo Passeri (more than 19 000 events over 2018-2024)
- Regression of the number of one-month $(t+1)$ events on the previous month t (should be independent for a Poisson process model to be valid)



- Autocorrelation in other cyber-database (**PRC database**, see [BBH20])

Relaxing independence assumptions on claims arrivals

Self-exciting arrival of claims and clustering effects

- Hawkes process: self-exciting counting process with stochastic intensity, fully specified by the point process itself (equivalently its jump times $(\tau_n)_n$)
- Vast literature on Hawkes processes: (among many others)
  - in finance: LOB as in Bacry et al. (2013) or Rosenbaum et al. (2015), Credit risk as in Errais et al. (2013) or Bielecki et al. (2020)...
  - in insurance: Dassios and Zhao (2012), Magnusson (2015), Gao and Zhu (2018) ...
- H (linear) Hawkes process with
  - (deterministic) excitation kernel Φ
  - (deterministic) baseline intensity μ

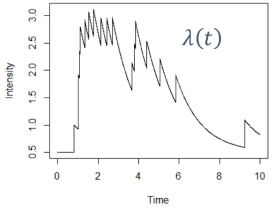
  is the counting process ($H_0 = 0$) with intensity process

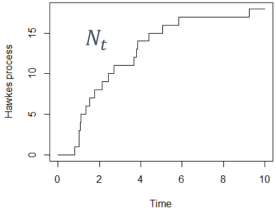
$$\lambda_t := \mu(t) + \int_{(0,t)} \Phi(t-s) dH_s = \mu(t) + \sum_{\tau_n < t} \Phi(t - \tau_n)$$

Hawkes Process with Exponential Kernel

Intensity of the Hawkes process with an exponential excitation kernel:

$$\lambda_t = \mu + \sum_{\tau_n < t} \alpha \exp\left(-\delta(t - \tau_n)\right)$$





- Each jump represents a cyber event.
- The intensity decays exponentially between jumps.

ENSAE
IP PARIS

Impact of the severity of the claims on the excitation kernel

Cumulative Loss process

$$L_t := \sum_{i=1}^{H_t} C_i, \quad t \in [0, T],$$

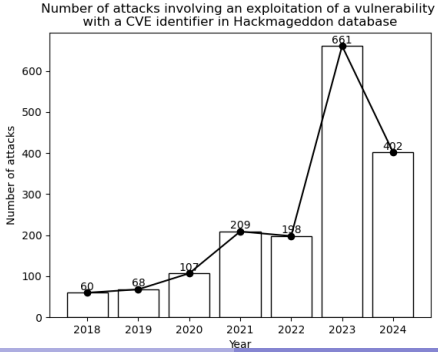
- Frequency: Claims arrival modeled by a Hawkes process H
- Impact of claims amounts on the excitation kernel : dependencies between the frequency component H and the severity component (claims amounts C_i)

$$\lambda_t := \mu(t) + \sum_{\tau_n < t} \Phi(t - \tau_n, C_n)$$

It could be $\Phi(t - \tau_n, C_n) = b(C_n)\phi(t - \tau_n)$ for a deterministic function b, ex: $b(c) = \mathbf{1}_{\{c \geq K\}}$.

External excitation

- The clustering feature not only due to contagion, but also to the arrival of external shocks such as **vulnerabilities** disclosures
- In Hackmageddon database : Number of cyber-attacks involving a vulnerability with a CVE identifier



Vulnerabilities and AI

Treasury and Fed alert major US banks in April 2026:

Risks linked to **Anthropic (Mythos)**, capable of detecting and exploiting flaws in their IT Systems.


Les Echos

Économie Politique Entreprises Finance - Marchés Bourse Monde Tech - Médias Start-up Régions Patrimoine Travailler mieux

IA : l'administration Trump alerte les banques face à la menace Mythos, le nouveau modèle d'Anthropic

Le Trésor américain et la Fed ont convoqué en urgence les grandes banques américaines pour évoquer la hausse du risque cyber lié au nouveau modèle d'Anthropic. Capable de détecter des failles critiques, cette technologie suscite des inquiétudes sur la cybersécurité du système financier.

Scott Bessent, secrétaire général du Trésor américain, devant le comité des services financiers à Washington le 4 février. (Photo Bonnie Cash/UPI/Abaca)

Stochastic baseline intensity

- Extension of Hawkes with stochastic baseline intensity μ
- The stochastic baseline intensity captures the impact of random external events, such as **vulnerabilities** disclosure

$$\lambda_t = \underbrace{\mu_0(t)}_{\text{deterministic part}} + \underbrace{\sum_{\tau_k^{ext}<t} \Phi^{ext}(t-\tau_k^{ext}, V_k)}_{\text{External shocks}} + \underbrace{\sum_{\tau_n^{int}<t} \Phi^{int}(t-\tau_n^{int}, C_n)}_{\text{Self-excitation}} \quad (1)$$

- External shocks (vulnerabilities) counting process $N_t^{ext} = \sum_{k\geq 1} \mathbf{1}_{\tau_k^{ext}\leq t}$ (Poisson process or self-exciting process)
- with severity marks $\{V_k\}_{k\geq 1}$ i.i.d. positive random variables
  - For cyber vulnerabilities: CVSS scores notified in the National Vulnerability Database
- **Calibration on Hackmaggedon and NVD databases, see Yousra's talk.**

Sample trajectory of intensity and cumulative loss

Multivariate self-exciting processes with dependencies

- A **more accurate**/flexible model (than Cramer-Lundberg) ...
  but **less tractable**
- How to compute formula for Risk Evaluation (such as expectation, correlation, expected surplus loss of stress scenarios, expected shortfall, insurance Stop Loss contracts...)?
  - For general kernels Φ (with spectral radius < 1)
  - In no stationary regimes
- Towards an unifying writing : Poisson imbedding also called Thinning Algorithm - Ogata (1981), Brémaud-Massoulié (1996) ...
  - A general class of processes: Multivariate self-exciting processes with dependencies
  - Multivariate version allows one to take into account risks with multivariate components, external excitation.
- Tools :
  - non-compensated Malliavin calculus, IPP formula (Last (2016))
  - Pseudo-chaotic expansion (developed in [HR24]).

ENSAE
IP PARIS

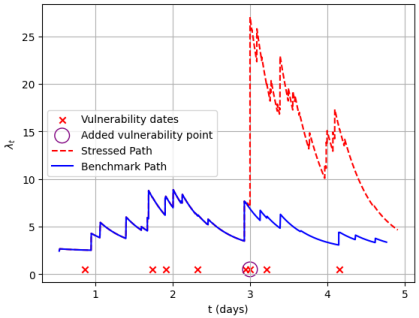
Stress Scenarios on a cyber portfolio

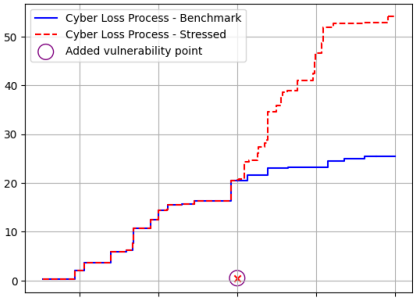
Cumulative portfolio loss:

$$L_t := \sum_{i=1}^{H_t} C_i, \quad t \in [0, T],$$

- Stress scenarios: Use of stochastic tools (addition operators) to mathematically inject deterministic shocks and generate stressed trajectories.
- Scenario stressed by $\mathcal{S}^p$ = Addition of p shocks $\{\mathbf{x}_1, \ldots, \mathbf{x}_p\}$ to the trajectory (with $\mathbf{x}_i := (t_i, y_i, k_i)$).
  - Additional claims in the portfolio: $k_i = 1$, $y_i = c_i$
  - Massive disclosure of critical vulnerabilities: $k_i = 2$, $y_i = v_i$

Stressed Trajectory





Hawkes intensity and cumulative loss trajectories
(Benchmark and Stressed)

Quantifying the Excess Loss Generated by Shocks

- In a "Poisson Process" model:

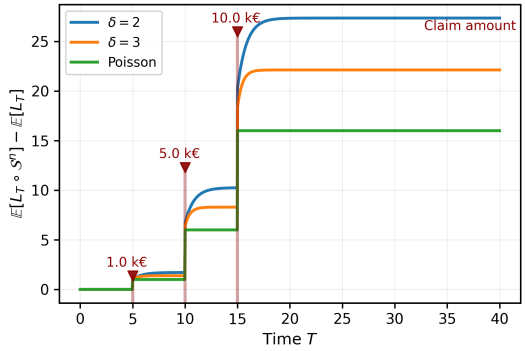
$$\mathbb{E}[L_T \circ \varepsilon_{S^p}^{+p}] - \mathbb{E}[L_T] = \sum_{j=1}^{p} c_j \mathbf{1}_{\{k_j=1\}}$$

- For the general model: additional terms due to the systemic nature (aftershocks)
- Calculation methodology: Combination of recent results from uncompensated Malliavin calculus (Mecke and Pseudo-chaos)
- Risk management (Closed-form formulas): Obtaining exact analytical results for the quantities of interest (covariances, excess losses in stress tests), without relying on simulations.

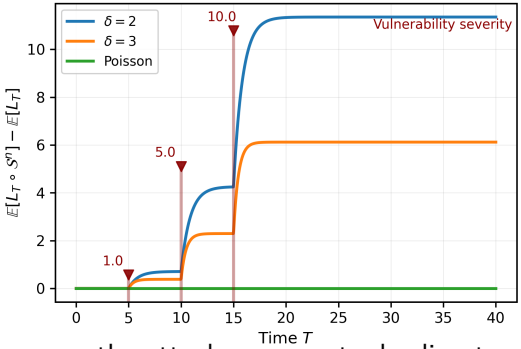
Stress Scenarios with Additional Claims

Exponential kernels, with parameters calibrated on real-world data.

λ_0	ρ	$\mathbb{E}(V_i)$	$\mathbb{E}(C_i)$	δ
3.10	84.79	0.12	0.83	2.37

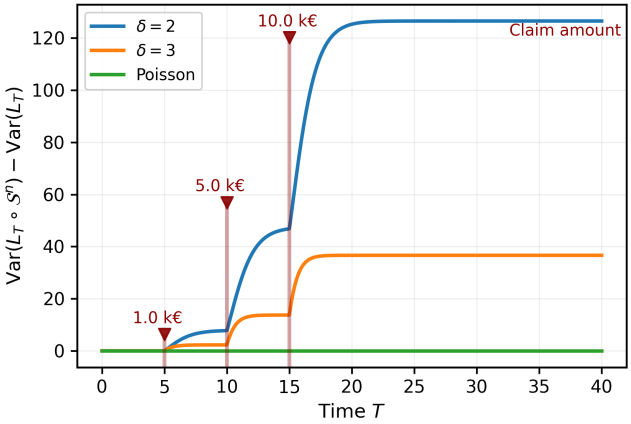


Stress Scenarios with Additional Vulnerabilities



- The lower δ is, the more the attacks propagate, leading to a higher loss surplus.
- In the absence of contagion in the model, the Poisson process underestimates the risk.

Variance of the Loss Surplus



Conclusion

- General model accounting for exogenous shocks and contagion phenomena, with complex dependencies.
- Quantification of the excess loss induced by these shocks: closed-form formulas for very broad classes of kernels, obtained using non-compensated Malliavin calculus tools and pseudo-chaotic decomposition.
- Possibility to also consider inhibition (beneficial technological shocks in terms of protection).
- Limitations:
  - Model calibration
  - Heterogeneity: classification of cyber-events using CART trees adapted for Hawkes process trajectories (work in progress).

Thank you for your attention.

ENSAE
IP PARIS

References

Cherkaoui, Y., Hillairet C., Peyrat, M., Reveillac A. (2026) **Stress scenarios of cyber loss processes with dependencies**, *https://cnrs.hal.science/ENSAE/hal-05558990v1*

Boumezoued A., Cherkaoui, Y., Hillairet C., (2025) **Cyber Risk Frequency Modelling Using Hawkes Processes: Calibration on Attack and Vulnerability Data**, *hal.science hal-05305048*

Hillairet C., Peyrat, M., Reveillac A. (2025) **Multivariate Self-Exciting Processes with Dependencies**, *https://arxiv.org/abs/2503.15958*

Bessy-Roland Y., Boumezoued A., Hillairet C., (2021) **Multivariate Hawkes process for Cyber Risk Insurance** in *Annals of Actuarial Science, Volume 15 Issue 1*

Hillairet C., Reveillac A., Rosenbaum M., (2021) **An expansion formula for Hawkes processes and application to cyber-insurance derivatives**, *Stochastic Processes and their Applications*