A stochastic Gordon-Loeb model for optimal security investment under clustered cyber-attacks

G. Callegaro [1] C. Fontana [1] C. Hillairet [2] B. Ongarato [3]

[1]University of Padova [2]ENSAE-CREST Paris
[3]TU Dresden

23rd Winter School on Mathematical Finance

Soesterberg, The Netherlands, 19-21 January 2026

Overview

Cyber-risk

Definition [Institute of Risk Management]: *any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems.*

Image source: ENISA Threat Landspace report (2024).

Facts on cyber-risk in Europe

- ENISA Threat Landscape report (2025)
  - Public Administration is the most targeted sector in the EU (38.5%)
  - The transport sector came in second (7.5%), with most reported incidents in air and logistics, with a focus on the maritime sector
  - Phishing was the dominant intrusion vector, accounting for approx. 60% of cases, followed by exploitation of vulnerabilities (21.3%)
  - At least 88 hacktivist groups claimed they targeted EU organisations. Pro-Russia nexus hacktivist groups remain prevalent, with 63.1% of attacks.
- AON 10th Global Risk Management Survey (2025):
  - Cyber attack or data breach tops the global agenda – again – remaining the number one current and future risk for the third time.

Never/ever happened to you?

Question: How do I know if it is a ransomware attack?

- ⋆ You will not be able to access your device or the data on it: the files are encrypted.
- ⋆ Usually you are asked to contact the attacker via an anonymous email address to make a payment in a cryptocurrency.

Recent attacks - The Netherlands:

- January 2025: no classes and exams postponed after cyberattack on Eindhoven University of Technology. The university took its systems offline for a week. Attackers had been active on the network for five days: they exploited leaked account credentials to log in via the VPN connection.
- June 2025: International Criminal Court was the target of a ‘sophisticated and targeted’ cyberattack. The ICC did not disclose whether sensitive information was stolen or who was behind the attack but stated that the attack had been stopped in time.

In the Netherlands ... [1]

- Increasingly complex threat assessment due to increasing cyber capabilities worldwide;
- Digital dependencies, resulting from geopolitical developments, increase the risk;
- Generative AI amplifies existing threats to digital security;
- No data on average losses;
- In 2024, there were at least 121 unique ransomware incidents in the Netherlands (147 in 2023) - source the National Cyber Security Centre (NCSC), the Police, the Public Prosecution Service (OM), Cyberveilig Nederland;
- Cybercriminals are not using new techniques to deploy ransomware;
- Criminals most often still gain access through software vulnerabilities and by taking over accounts.

[1] Source: Cybersecurity Assessment Netherlands 2025, `https://english.nctv.nl/documents/2025/12/02/cybersecurity-assessment-netherlands-2025`

Which challenges?

Citing Zeller et al. (2022), [15]:

- Limited availability and incomplete nature of data [2]
- Dynamic and constantly evolving risk type
- Interdependence/accumulation risk
- Difficult monetary impact determination.

[2] An excellent data analysis is present in the PhD thesis by Yousra Cherkaoui, Institut Polytechnique de Paris. Dataset used: Hackmageddon (date, type, category, geographic area, sector), containing exploited vulnerabilities.

Which challenges?

Citing Zeller et al. (2022), [15]:

- Limited availability and incomplete nature of data [2]
- Dynamic and constantly evolving risk type
- Interdependence/accumulation risk
- Difficult monetary impact determination.

[2] An excellent data analysis is present in the PhD thesis by Yousra Cherkaoui, Institut Polytechnique de Paris. Dataset used: Hackmageddon (date, type, category, geographic area, sector), containing exploited vulnerabilities.

What do we do here?

Key questions:

- How to describe in a realistic way the arrival of cyber-attacks?
- How to reduce losses from cyber-attacks by investing in cyber-security?
- How to determine the optimal investment in cyber-security?

What do we do here?

Key questions:

- How to describe in a realistic way the arrival of cyber-attacks?
- How to reduce losses from cyber-attacks by investing in cyber-security?
- How to determine the optimal investment in cyber-security?

Our contributions:

- Introduce a **continuous-time** model based on **Hawkes processes**;
- Develop a **stochastic version of the Gordon-Loeb model**;
- Formulate the problem as a **stochastic optimal control problem**;
- **Numerical solution and analysis**, to evaluate the optimal investment in cyber-security and the associated reduction of IT vulnerability.

The Gordon-Loeb model (2002)

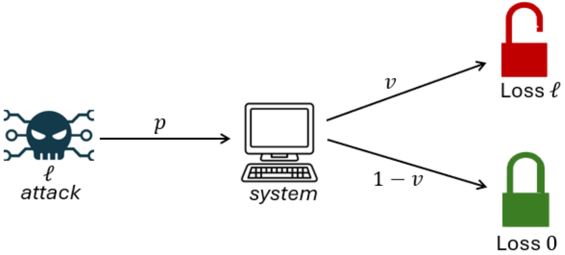
The basics

Aim: Determine the optimal amount to invest in security to protect an IT system.

Key ingredients:

- $p \in [0, 1]$: the probability that an attack occurs;
- $\ell > 0$: the potential loss;
- $v \in [0, 1]$: the vulnerability of the IT system, i.e., the probability of an attack to penetrate into the system (breach).

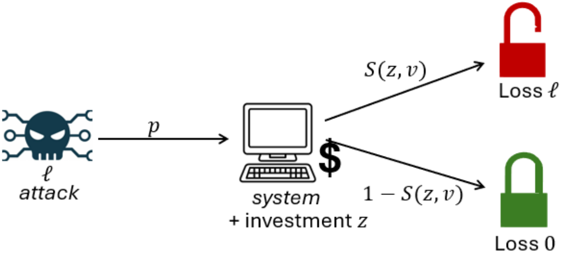
The expected loss is $\ell \mathbf{pv}$.



The Gordon-Loeb model

The security breach probability function

- The entity can invest an amount z in IT security.
- Investment z reduces the vulnerability;
- **Security breach probability function**: $S(z, v) < v$, in $[0, 1]$.



Assumptions on S

(A1) $S(z, 0) = 0$ for all z: an invulnerable system remains invulnerable.

(A2) For all v, $S(0, v) = v$: if no investment then the vulnerability remains equal to v.

(A3) For all $v \in (0, 1)$ and all z, $S_z(z, v) < 0$ and $S_{zz}(z, v) > 0$.

The Gordon-Loeb model

Examples of security breach probability functions

$$S_I(z, v) = \frac{v}{(az + 1)^b} \qquad \text{and} \qquad S_{II}(z, v) = v^{az+1}.$$

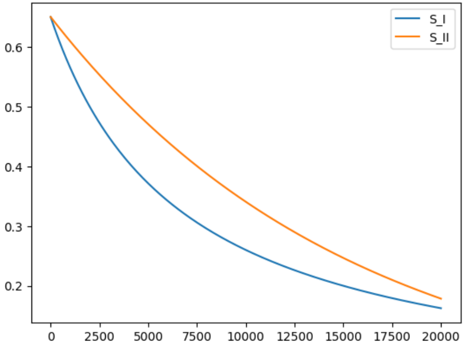


Figure: $v = 0.65$, $a = 1.5 \cdot 10^{-5}$, $b = 1$.

The Gordon Loeb model

Optimal investment and ENBIS

They max the Expected Net Benefit of Investment in Information Security:

Cost-benefit trade-off

$$\sup_{z \geq 0} \left\{ \big(v - S(z,v)\big) p\ell - z \right\}.$$

Solution:

- Optimal investment: z such that $-S_z(z,v)p\ell = 1$.
- For the two standard S seen before, $S_I(z,v) = \frac{v}{(az+1)^b}$ and $S_{II}(z,v) = v^{az+1}$, it holds that

$$z^*(v) < \frac{1}{e} v p\ell \quad \approx \quad \boxed{\text{37\% of the expected losses}}$$

The Gordon-Loeb Model

Comments and extensions

- Very simple model (no dynamicity, no stochasticity).
- ... Yet interesting! It provides a benchmark for security investments.

Some extensions

- More sophisticated security breach functions: Huang and Behara (2013), [7].
- Dynamic with a real option approach: Tatsumi and Goto (2010), [13].
- Applications to cyber-insurance: Young et al. (2016), [14], Mazzoccoli and Naldi (2020), [9], Skeoch (2022), [12].

Our extension:

A continuous-time version with randomly arriving, and clustered, attacks and random losses.

Modelization of cyber-attacks

Hawkes processes

- Evidence of **contagion and clustering** in cyber-attacks:
  the occurrence of an attack increases the likelihood of further attacks;
- Empirical evidence on the **self-exciting** behavior of cyber-attacks:
  - Baldwin et al. (2017): SANS Institute database, threats to Internet services;
  - Bessy-Roland et al. (2021): Privacy Rights Clearinghouse database;
  - Boumezoued et al. (2023): three different vulnerabilities databases.

Modelization of cyber-attacks

- Evidence of **contagion and clustering** in cyber-attacks: the occurrence of an attack increases the likelihood of further attacks;
- Empirical evidence on the **self-exciting** behavior of cyber-attacks:
  - Baldwin et al. (2017): SANS Institute database, threats to Internet services;
  - Bessy-Roland et al. (2021): Privacy Rights Clearinghouse database;
  - Boumezoued et al. (2023): three different vulnerabilities databases.
- **Hawkes process**: counting process with a self-exciting intensity

Definition (Hawkes process)

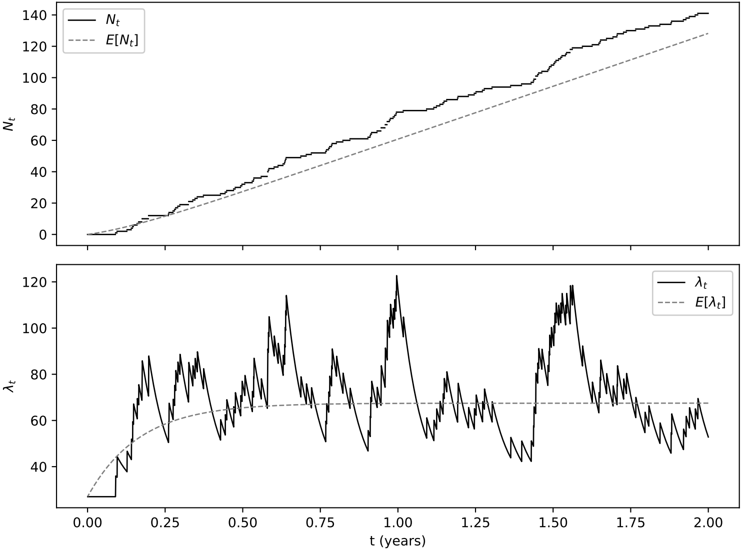
N is a counting process with stochastic intensity λ given by

$$d\lambda_t = -\xi(\lambda_t - \alpha)dt + \beta dN_t, \qquad \lambda_0 > 0,$$

or

$$\lambda_t = \alpha + (\lambda_0 - \alpha)e^{-\xi t} + \beta \sum_{n=1}^{N_t} e^{-\xi(t-\tau_n)}.$$

One trajectory ($\alpha = 27$, $\lambda_0 = 27$, $\xi = 15$, $\beta = 9$)



Our proposal

A dynamic version of the Gordon-Loeb model

On $(\Omega, \mathcal{F}, \mathbb{P})$

1. $(\tau_i)_{i\in\mathbb{N}}$: arrival times of cyber-attacks
2. N: counting process $N_t = \sum_{i=1}^{+\infty} \mathbb{1}_{\{\tau_i \leq t\}}$
3. η_i: the potential random loss induced by the i-th attack, $\mathbb{E}[\eta_i] = \bar{\eta}$
4. $(z_t)_{t\in[0,T]}$: investment rate in security (control process)
5. ρ decaying factor and H cumulative investment

$$H_t = H_0 e^{-\rho t} + \int_0^t e^{-\rho(t-s)} z_s \mathrm{d}s, \quad t \in [0, T].$$

6. Losses:

Potential losses	Losses without investment	Losses with investment
$C_t = \sum_{i=1}^{N_t} \eta_i$	$L_t^0 = \sum_{i=1}^{N_t} \eta_i \cdot B_i^v$	$L_t^z = \sum_{i=1}^{N_t} \eta_i \cdot B_i^{S(H_{\tau_i}, v)}$
	$B_i^v \sim \mathrm{Be}(v)$, i.i.d.	$B_i^{S(h,v)} \sim \mathrm{Be}\left(S(h, v)\right)$

The optimization problem

In the spirit of the Gordon-Loeb model:

$$\sup_{z \in \mathcal{Z}} \mathbb{E}\left[\overbrace{L_T^0 - L_T^z}^{\text{benefit}} \underbrace{- \left(\int_0^T z_t + \frac{\gamma}{2} z_t^2 \mathrm{d}t \right)}_{\text{quadratic cost}} + \overbrace{U(H_T)}^{\text{terminal utility}} \right]$$

$$= \sup_{z \in \mathcal{Z}} \mathbb{E}\left[\int_0^T \left(\overbrace{(v - S(H_t, v))\bar{\eta}\lambda_t}^{\text{benefit}} \underbrace{- z_t - \frac{\gamma}{2} z_t^2}_{\text{quadratic cost}} \right) \mathrm{d}t + \overbrace{U(H_T)}^{\text{terminal utility}} \right].$$

$$\mathrm{d}\lambda_t = -\xi(\lambda_t - \alpha)\mathrm{d}t + \beta \mathrm{d}N_t, \quad \lambda_0 > 0$$
$$\mathrm{d}H_t = (-\rho H_t + z_t)\mathrm{d}t, \quad H_0 > 0.$$

- $\mathcal{Z} = \{(z_t)_{t \in [0,T]}$: $z_t \geq 0$, adapted w.r.t. $\mathbb{F} = (\mathcal{F}_t)_{t \in [0,T]}$, $\mathcal{F}_t = \sigma(N_s, s \leq t)$ and $\mathbb{E}\left[\int_0^T z_t^2 \mathrm{d}t\right] < \infty\}$.
- $U(H_T)$: utility of IT cumulated security investment at T.

Value function and optimal control

$$V(t,\lambda,h) = \sup_{z\in\mathcal{Z}_t} \overbrace{\mathbb{E}\left[\int_t^T \left((v - S(H_s^{t,h,z}, v))\bar{\eta}\lambda_s^{t,\lambda} - z_s - \frac{\gamma}{2} z_s^2\right) \mathrm{d}s + U(H_T^{t,h,z})\right]}^{J(t,\lambda,h;z)}$$

- Hamilton-Jacobi-Bellman equation:

$$\frac{\partial V}{\partial t} - \xi(\lambda - \alpha)\frac{\partial V}{\partial \lambda} - \rho h \frac{\partial V}{\partial h} + \lambda(V(t,\lambda+\beta,h) - V(t,\lambda,h)) + (v - S(h,v))\bar{\eta}\lambda$$
$$+ \frac{\left(\frac{\partial V}{\partial h} - 1\right)^+}{\gamma}\left(\frac{\partial V}{\partial h} - 1 - \frac{\gamma}{2}\frac{\left(\frac{\partial V}{\partial h} - 1\right)^+}{\gamma}\right) = 0, \quad V(T,\lambda,h) = U(h).$$

- Optimal control

$$z_t^* = \frac{\left(\frac{\partial V}{\partial h}(t,\lambda_t,H_t) - 1\right)^+}{\gamma}.$$

Algorithm Numerical scheme based on the Method Of Lines

1: Choose $\lambda_{min}, \lambda_{max}, h_{min}, h_{max}$.
2: Discretize $[\lambda_{min}, \lambda_{max}]$, $\lambda_0 = \lambda_{min}, \lambda_N = \lambda_{max}$, $\lambda_n - \lambda_{n-1} = \Delta\lambda$.
3: Discretize $[h_{min}, h_{max}]$, $h_0 = h_{min}, h_M = h_{max}$, $h_m - h_{m-1} = \Delta h$.
4: Define $V_{n,m}(t) := V(t, \lambda_n, h_m)$.
5: Approximate the partial derivatives w.r.t. λ: $\frac{\partial V}{\partial \lambda}(t, \lambda_n, h_m) \approx \frac{V_{n,m}(t) - V_{n-1,m}(t)}{\Delta\lambda}$.
6: Approximate the partial derivatives w.r.t. h: $\frac{\partial V}{\partial h}(t, \lambda_n, h_m) \approx \frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h}$.
7: Let $\tilde{n} = \frac{\lfloor \beta \rfloor}{\Delta\lambda}$, $V(t, \lambda_n + \beta, h_m) \approx V_{(n+\tilde{n})\wedge N,m}(t)$.
8: Solve using an ODE solver the system given for every n, m by

$$V'_{n,m}(t) = \xi(\lambda_n - \alpha)\frac{V_{n,m}(t) - V_{n-1,m}(t)}{\Delta\lambda} + \rho h \frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h}$$
$$- \lambda_n(V_{n+\tilde{n}\wedge N,m}(t) - V_{n,m}(t)) - (v - S(h_m, v))\bar{\eta}\lambda_n$$
$$- \frac{\left(\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} - 1\right)^+}{\gamma}\left(\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} - 1 - \frac{\gamma}{2}\frac{\left(\frac{V_{n,m+1}(t) - V_{n,m}(t)}{\Delta h} - 1\right)^+}{\gamma}\right),$$
$$V_{n,m}(T) = U(h_m).$$

Numerical results

Parameters

S	v	a	b
S_I	0.65	0.1	1

Table: Security breach function, Skeoch, H. R. (2022), [12].

α	ξ	β	λ_0
27	15	9	27

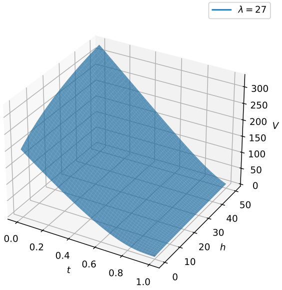
Table: Hawkes intensity, Boumezoued et al. (2023), [5]. Intuition: 60 attacks on average per year.

Optimization	γ	$\bar{\eta}$(k\$)	$U(h)$	ρ	T
	0.05	10	$\sqrt{h}$	0.2	1

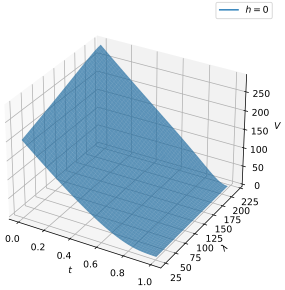
Table: Optimization problem parameters.

Numerical results

Value function $V(t, \lambda, h)$



(a) Value function for $\lambda = 27$.

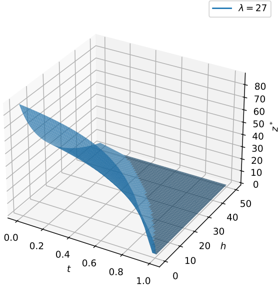


(b) Value function for $h = 0$.

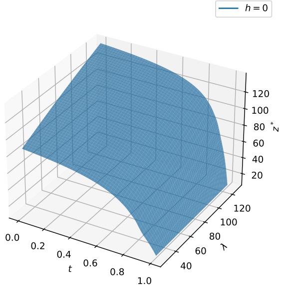
- **Increasing in** h: larger initial investment $\longrightarrow$ greater benefit.
- **Increasing in** λ: larger risk $\longrightarrow$ larger benefit.
- **Decreasing in** t: investment is less relevant near T.

Numerical results

Optimal control $z_t^*(\lambda, h)$



(a) Optimal control for $\lambda = 27$.



(b) Optimal control for $h = 0$.

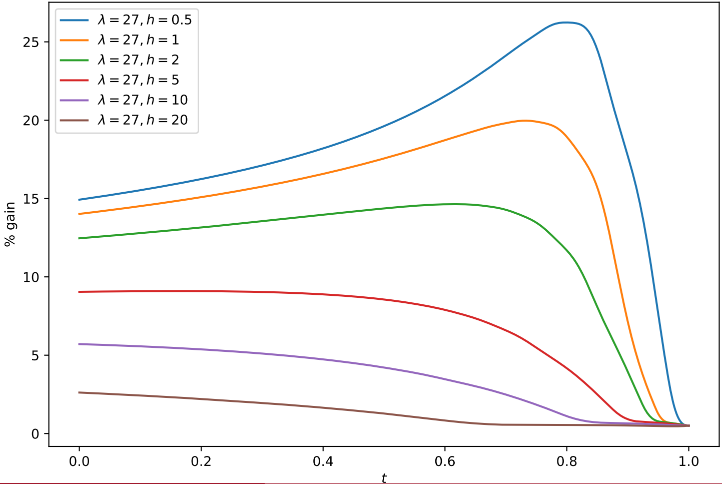
- **Decreasing in** h: larger initial investment $\longrightarrow$ smaller investment.
- **Increasing in** λ: larger risk $\longrightarrow$ larger investment.
- **Decreasing in** t: investment is less relevant near T.

Numerical results

Comparison with a constant investment strategy

We choose $z_t \equiv \bar{z}^*$ solving $J(t,\lambda,h;\bar{z}^*) = \sup_{\bar{z}\in\mathbb{R}_+} J(t,\lambda,h;\bar{z})$ and we plot

$$\text{gain} := 100 \times \frac{V(t,\lambda,h) - J(t,\lambda,h;\bar{z}^*)}{J(t,\lambda,h;\bar{z}^*)}$$



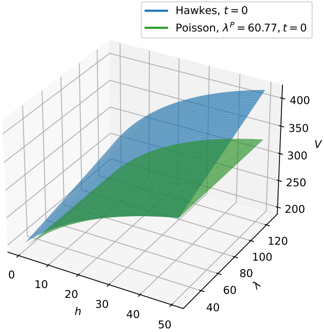
Numerical results

Comparison with standard Poisson P

Consider P for the arrival of cyber-attacks, with constant λ^P s.t. $\mathbb{E}[P_T] = \mathbb{E}[N_T]$:

$$\lambda^P = \frac{\lambda_0 \xi}{\xi - \beta} + \frac{1 - e^{-\xi T}}{T(\xi - \beta)} \left(\lambda_0 - \frac{\lambda_0 \xi}{\xi - \beta} \right) \approx 60.77.$$

Idea: The myopic firm correctly estimates the intensity, on average.
Value functions: Hawkes (blue) / Poisson (green)



Numerical results

Comparison with Poisson along a trajectory

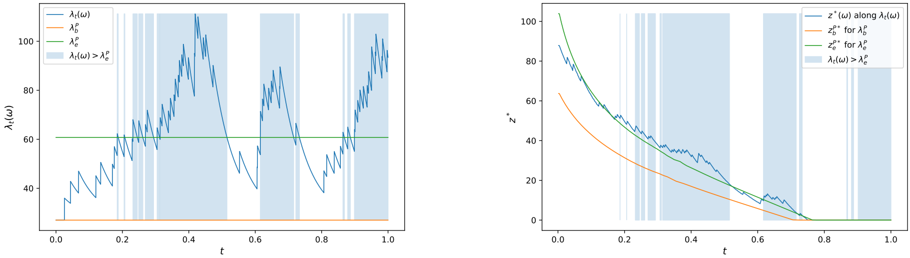


Figure: Intensity trajectory (left) and optimal control (right).

Conclusions and outlook

- Continuous-time stochastic version of the Gordon-Loeb model;
- Arrival process of cyber-attacks with clustering behavior;
- Evidence of the impact of randomly arriving cyber-attacks;
- More (numerical) results in the paper!

Next steps:

- Rigorous theoretical analysis of the stochastic optimal control problem;
- Introduction of cyber-insurance;
- Calibration of the model to real data.

Grazie!

Paper available on https://arxiv.org/abs/2505.01221!

References I

- Baldwin, A., Gheyas, I., Ioannidis, C., Pym, D., & Williams, J. (2017). Contagion in cyber security attacks. Journal of the Operational Research Society, 68(7), 780-791.
- Bensalem, S., Hernández-Santibáñez, N., & Kazi-Tani, N. (2023). A continuous-time model of self-protection. Finance and Stochastics, 27(2), 503-537.
- Bessy-Roland, Y., Boumezoued, A., & Hillairet, C. (2021). Multivariate Hawkes process for cyber insurance. Annals of Actuarial Science, 15(1), 14-39.
- Bouchard, B. (2007). Introduction to stochastic control of mixed diffusion processes, viscosity solutions and applications in finance and insurance. Lecture Notes Preprint.
- Boumezoued, A., Cherkaoui, Y., & Hillairet, C. (2023). Cyber risk modeling using a two-phase Hawkes process with external excitation. arXiv preprint arXiv:2311.15701.

References II

- Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5(4), 438-457.
- Huang, C. D., & Behara, R. S. (2013). Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints. International Journal of Production Economics, 141(1), 255-268.
- Jang, J., & Oh, R. (2021). A review on Poisson, Cox, Hawkes, shot-noise Poisson and dynamic contagion process and their compound processes. Annals of Actuarial Science, 15(3), 623-644.
- Mazzoccoli, A., & Naldi, M. (2020). Robustness of optimal investment decisions in mixed insurance/investment cyber risk management. Risk analysis, 40(3), 550-564.
- Miaoui, Y., & Boudriga, N. (2019). Enterprise security economics: A self-defense versus cyber-insurance dilemma. Applied Stochastic Models in Business and Industry, 35(3), 448-478.

References III

Øksendal, B., & Sulem, A. (2005). Applied Stochastic Control of Jump Diffusions, Springer International Publishing.

Skeoch, H. R. (2022). Expanding the Gordon-Loeb model to cyber-insurance. Computers & Security, 112, 102533.

Tatsumi, K. I., & Goto, M. (2010). Optimal timing of information security investment: A real options approach. In Economics of information security and privacy (pp. 211-228). Boston, MA: Springer US.

Young, D., Lopez Jr, J., Rice, M., Ramsey, B., & McTasney, R. (2016). A framework for incorporating insurance in critical infrastructure cyber risk strategies. International Journal of Critical Infrastructure Protection, 14, 43-57.

Zeller, G., & Scherer, M. (2022). A comprehensive model for cyber risk based on marked point processes and its application to insurance. European Actuarial Journal, 12(1), 33-85.