Accumulation of cyber claims: modeling contagion

Caroline Hillairet, **Olivier Lopez**
Sorbonne Université, Paris
Joint Research Initiative "Cyber insurance: actuarial modeling"
(AXA Research Fund, Ensae, Sorbonne Université, Risk Fundation)

ASTIN online Colloquium

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Cyber-risk

- Cyber-risk: inappropriate use of numerical tools and information systems.
- A cyber incident can be voluntary (cyber attack) or not (accidents may happen).
- For hacking, hackers use vulnerabilities in information systems, from outside or from inside.
- Various types of attacks (ransomware, phishing, classic frauds...)
- Strike states, companies, people.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

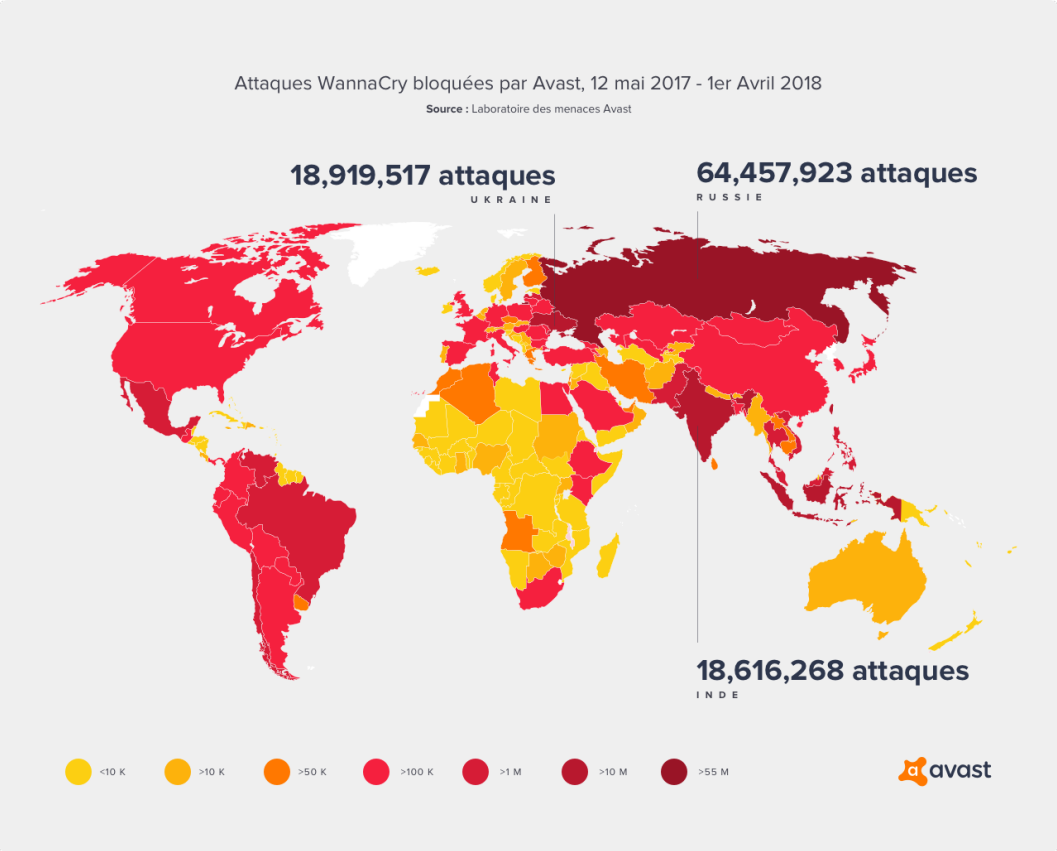
Wannacry

- Ransomware Wannacry : worldwide cyber attack in May 2017.
- Use the vulnerability "EternalBlue".
- Approximatively 200 000 infected computers across 150 countries over approximatively one week.
- Estimation of the cost : hundreds of million dollars, billions according to some estimations. ($100 millions for the NHS).

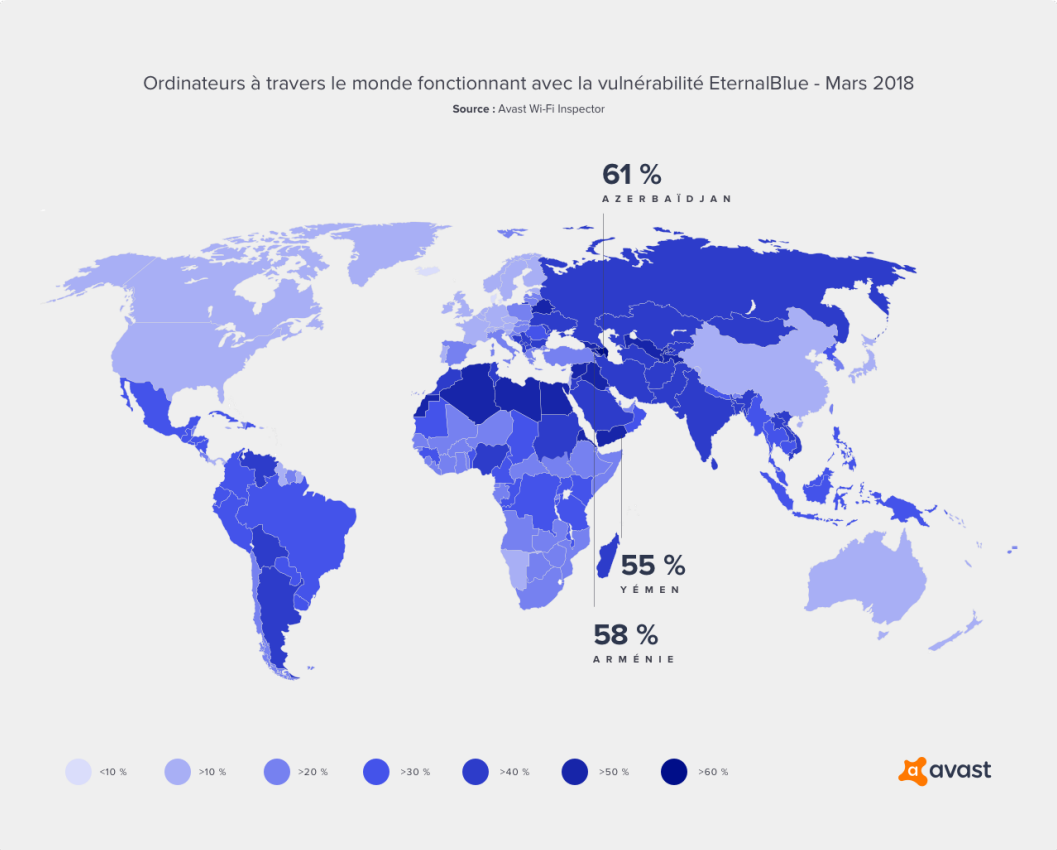
SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Wannacry in maps



Wannacry in maps



Covid-19

- Increased use of digital tools.
- Increase of teleworking, often without fully secured methods (mix of personal and professional tools).
- Waves of attacks taking advantage of the Covid-19 crisis: Cyber-Threat Covid-19 coalition identified approximatively 26 000 URL or malicious websites related to Covid-19 during April 2020.
- All the classical types of attacks have increased during this period, see for example *Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic* by Kahn et al. : `https://www.techrxiv.org/articles/Ten_Deadly_Cyber_Security_Threats_Amid_COVID-19_Pandemic/12278792\T1\o`

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Cyber insurance market (France)

- CESIN (annual French barometer for cyber-security):
  - 80% of organisations were targeted by at least one cyber-attack in 2018,
  - with damages (like business interruption) more significant than in 2017.

Cyber insurance market (France)

- CESIN (annual French barometer for cyber-security):
  - 80% of organisations were targeted by at least one cyber-attack in 2018,
  - with damages (like business interruption) more significant than in 2017.

- Cyber-insurance (Opinion Way for CESIN in 2017):
  - 40% of organisations had subscribed (25% in 2016),
  - 37% were in the process of subscribing or willing to (17% in 2016).

Cyber insurance market (France)

- CESIN (annual French barometer for cyber-security):
  - 80% of organisations were targeted by at least one cyber-attack in 2018,
  - with damages (like business interruption) more significant than in 2017.

- Cyber-insurance (Opinion Way for CESIN in 2017):
  - 40% of organisations had subscribed (25% in 2016),
  - 37% were in the process of subscribing or willing to (17% in 2016).

- Cyber-insurance challenges:
  - wording: affirmative/silent cover,
  - risk mitigation, Claims handling,
  - actuarial modeling,
  - accumulation risk.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Outline

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Outline

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

The approach

- Objectives
  - To model and control the dynamics of the infected policyholders in an insurance portfolio
  - To quantify and calibrate the implementation of countermeasures.
- Model composed of three modules :
  - environment module : the global dynamic of the cyber event (that can be described through compartmental epidemiological models)
  - repair/assistance module : duration of the assistance required
  - prevention and response module : reactivity in detecting the incident and to implement countermeasures.
- Help for an insurance company to quantify
  - how much should be the response capacity in order to sufficiently reduce the impact of a given scenario
  - how much is won if one increases the capacity of response (to fix the price of a partnership with a cyber security firm).

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

The general model

- $t = 0$: start of the cyber-epidemic

Micro modeling of the cyber-epidemic

For a policyholder, we define

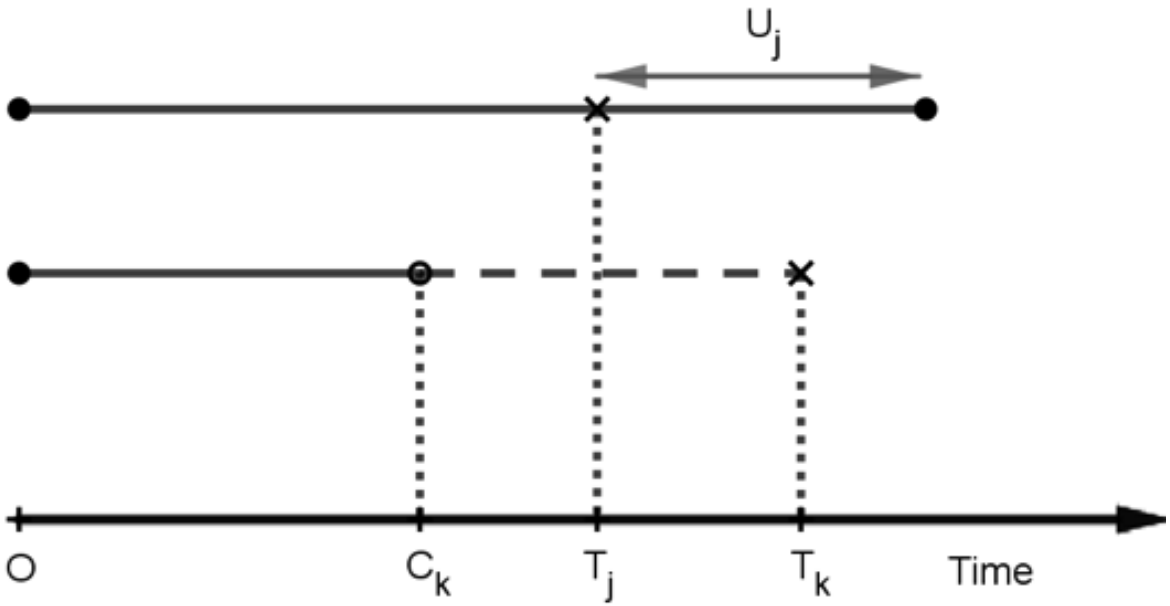
- T = Time of infection (possibly equal to $+\infty$),
- U = Duration of the assistance required after infection,
- C = Time at which policyholder becomes immune.

- Policyholders are assumed independent (contagion comes from outside the portfolio).
- We assume T independent of C.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Chronology of the cyber events



Three variables to be modeled

- Module "environment" : T models the severity of the infection in the global population (epidemiological model).
- Module "repair" : U depends of the type of infection (ransomware, malware, data-corruption...). It is the duration of immediate assistance.
- Module "prevention and response" : C describes the ability to react to the crisis, the reactivity to identify the incident and to implement countermeasures.
- See Hillairet, Lopez (2021), *Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models*, **Scandinavian Actuarial Journal**.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Hazard rate function

- Hazard rate function is a natural quantity to model duration variables.
- Definition :

$$\lambda_T(t) = \lim_{dt \to 0^+} \frac{1}{dt} \mathbb{P}(T \in [t, t+dt] | T \geq t).$$

- Link with the density function f_T and the survival function $S_T = \mathbb{P}(T \geq t)$:

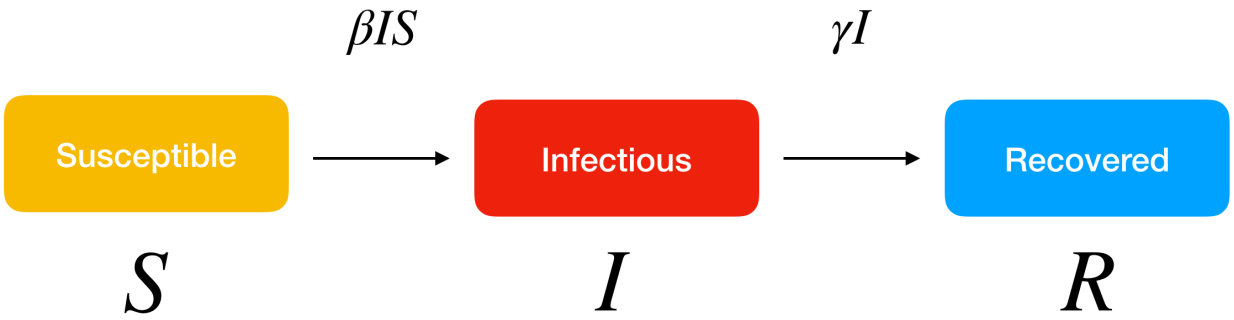
$$\lambda_T(t) = \frac{f_T(t)}{S_T(t)}.$$

- For the variable T, λ_T is "calibrated" using a SIR model (but other models are possible).

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

SIR model



- The population in the three compartments evolves through the following system of differential equations:

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

From SIR to λ_T

- Number of susceptible at time t : $S(t)$.
- Number of new infections between t and $t + dt$: $\beta S(t)I(t)$.
- The probability for a policyholder to be infected between t and $t + dt$ (given that he has not been infected before t) is

$$\frac{\beta S(t)I(t)}{S(t)} = \beta I(t).$$

- Conclusion :

$$\lambda_T(t) = \lim_{dt \to 0^+} \frac{1}{dt} \mathbb{P}(T \in [t, t + dt] | T \geq t) = \beta I(t).$$

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

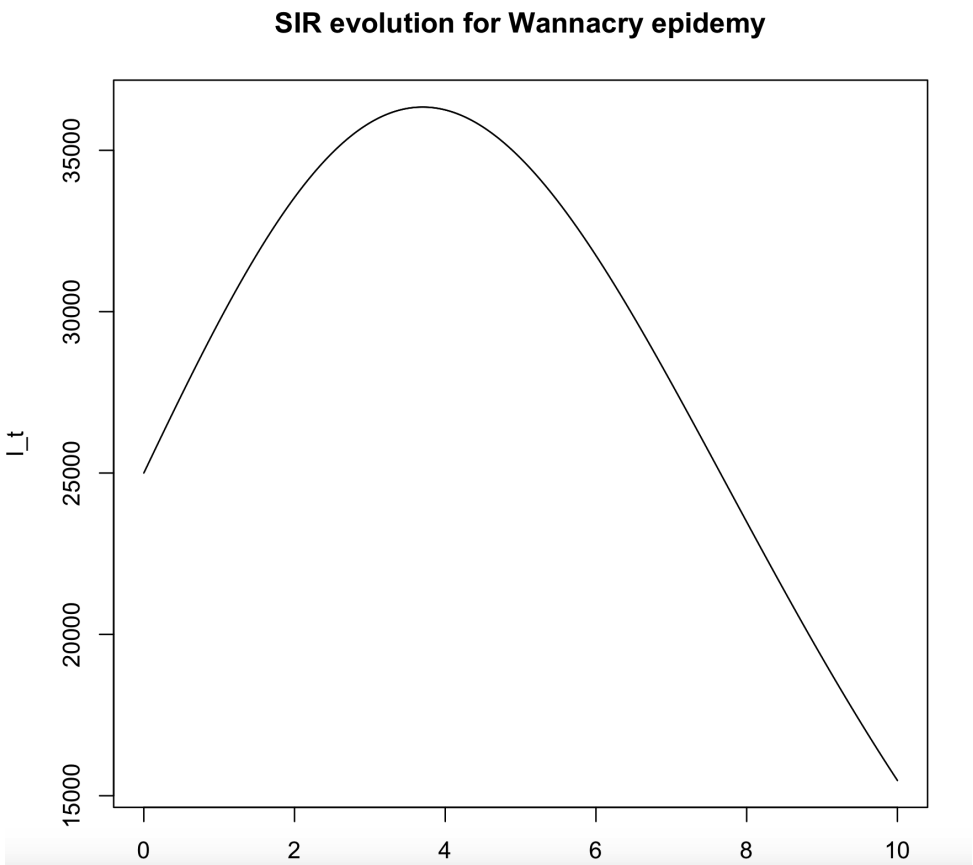
Calibration

- Difficult calibration of SIR model in cyber epidemic (few available data).
- What is a reasonable β, and what is the exposure N in the global population?
- What do we know on Wannacry :
  - the total number of infected
  - the duration of the epidemic
  - the dynamics of the ransom payments (using bitcoins addresses used to pay the ransoms).

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Example of epidemic dynamics of Wannacry type

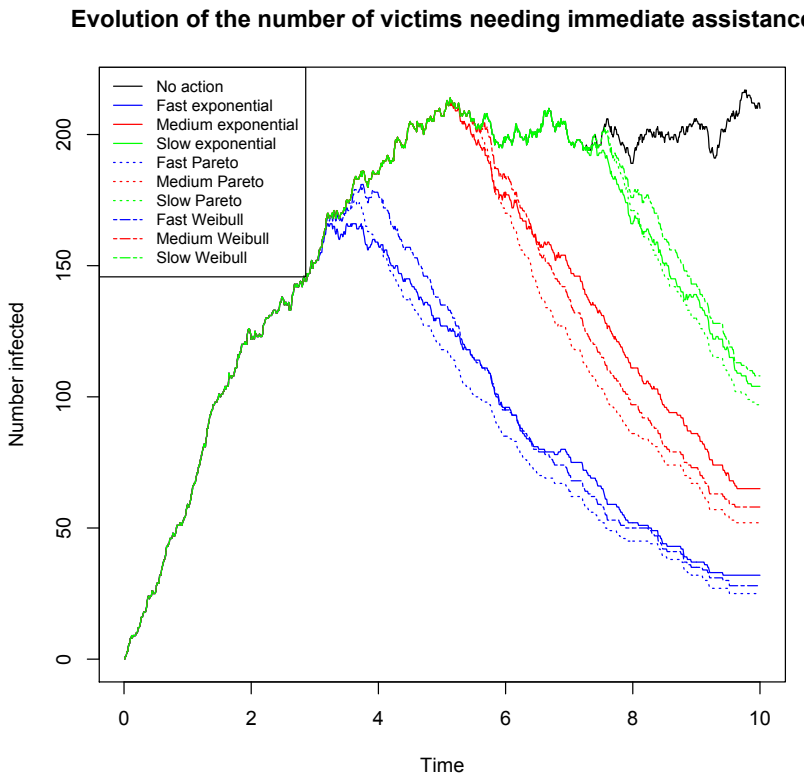


What can we quantify with this model ?

- One can quantify :
  - the total number of infected policyholders on each scenario;
  - its evolution, and thus the impact of the different reactions ;
  - the risk of "saturation", i.e. the risk that the insurer is not able anymore to provide the promised technical assistance to his policyholders.

Simulation of a Wannacry-type scenario

- Simulation on a portfolio of 10 000 policyholders.



SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Outline

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Multi-group SIR models

- Multi-group SIR: consider B subpopulations:

$$\frac{dS_i(t)}{dt} = -\left\{\sum_{j=1}^{B} \beta_{i,j} I_j(t)\right\} S_i(t)$$

$$\frac{dI_i(t)}{dt} = \left\{\sum_{j=1}^{B} \beta_{i,j} I_j(t)\right\} S_i(t) - \gamma_i I_i(t)$$

$$\frac{dR_i(t)}{dt} = \sum_{i=1}^{B} \gamma_i I_i(t).$$

- $\beta_{i,j}$ materializes how j contaminates i.
- Allows to introduce network effects.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Multi-group SIR models

- Multi-group SIR: consider B subpopulations:

$$\frac{dS_i(t)}{dt} = -\left\{\alpha_i(t) + \sum_{j=1}^{B} \beta_{i,j} I_j(t)\right\} S_i(t)$$

$$\frac{dI_i(t)}{dt} = \left\{\alpha_i(t) + \sum_{j=1}^{B} \beta_{i,j} I_j(t)\right\} S_i(t) - \gamma_i I_i(t)$$

$$\frac{dR_i(t)}{dt} = \sum_{i=1}^{B} \gamma_i I_i(t).$$

- $\alpha_i(t)$ represents an intensity of attacks in class i.
- Example: single initial burst $\alpha_i(t) = \alpha \mathbf{1}_{0 \le t < 1}$ for some i.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Multi-group SIR models

- Multi-group SIR: consider B subpopulations:

$$\frac{dS_i(t)}{dt} = -\left\{\alpha_i(t) + \eta_i(t)\sum_{j=1}^{B}\beta_{i,j}I_j(t)\right\}S_i(t)$$

$$\frac{dI_i(t)}{dt} = \left\{\alpha_i(t) + \eta_i(t)\sum_{j=1}^{B}\beta_{i,j}I_j(t)\right\}S_i(t) - \gamma_i I_i(t)$$

$$\frac{dR_i(t)}{dt} = \sum_{i=1}^{B}\gamma_i I_i(t).$$

- $\eta_i(t)$ represents how population i tends to protect itself against the threat.
- Example: $\eta_i(t) = \eta\mathbf{1}_{S_i(0)/S_i(t)\geq s}$.

Final number of victims

- $R_i(\infty)$ = final number of victims in class i, $\mathbf{R} = (R_1(\infty), ..., R_d(\infty))$.
- One can show that the vector $\mathbf{R}$ is the unique solution of a fixed point equation

$$\mathbf{R} = \Phi(\mathbf{R}),$$

where

$$\Phi_i(\mathbf{x}) = I_i(0) + S_i(0) \left\{ 1 - \exp\left(-\mathcal{A}_i - \sum_{k=1}^{d} \frac{\beta_{k,i}}{\gamma_i} x_k \right) \right\},$$

with $\mathcal{A}_i = \int_0^\infty \alpha_i(t)dt$.

- From $\mathbf{R}$, one deduces the probability of being hit for each category present in the portfolio.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

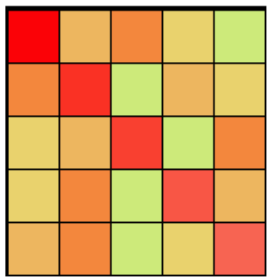
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Impact of the connectivity

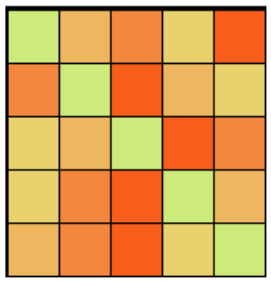
- We consider different classes of matrices $\mathcal{B}$ for the matrix B.
- Each class $\mathcal{B}$ has some properties, and we simulate random matrices from this class, and look at the final impact.
- Two examples:
  - "Clustered" : the transmission is essentially intern to a class.
  - "Non-clustered" : the transmission is stronger from one class to another than within a given class.

Two examples of matrices

- 5 classes.
- First class: 36% of the total population.
- 5-th class: 16% of the total population.
- Clustered:



- Non-clustered:



Comparison with a reference scenario

- Reference scenario: one single class, infection similar to Wannacry, initialization through an attack function $\alpha_1(t) = \alpha_0 \mathbf{1}_{0 \leq t \leq 1}$.
- Question: how much should we increase α to obtain the same number of victims as Wannacry depending on:
  - the class of matrices $\mathcal{B}$ (here "clustered", "non-clustered")?
  - the class in which the initial attack is performed?
- 100,000 simulations, $(E[\alpha] - \alpha_0)/\alpha_0$:

	Clustered	Non-Clustered
Attack on class 1	1.96	1.82
Attack on class 5	2.10	1.98

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

A first conclusion

- Through this short example:
  - if, at first, a single class is attacked, communities tend to slow down the infection.
  - the more the communities are "separated", the stronger should be the attack to achieve the same level.
  - otherwise (non-clustered case), after some point there is an outbreak in the majority class.
- Other classes of matrices: possibility to look at some different shapes of networks as in Fahrenwaldt, Weber, Weske (2018) **Pricing of cyber insurance in a network model,** *ASTIN Bulletin*.

A first conclusion

- Through this short example:
  - if, at first, a single class is attacked, communities tend to slow down the infection.
  - the more the communities are "separated", the stronger should be the attack to achieve the same level.
  - otherwise (non-clustered case), after some point there is an outbreak in the majority class.
- Other classes of matrices: possibility to look at some different shapes of networks as in Fahrenwaldt, Weber, Weske (2018) **Pricing of cyber insurance in a network model,** *ASTIN Bulletin*.
- To be investigated:
  - calibration of the network structure.
  - importance of the reaction (η_i in the differential system).
  - network effect on the "peak" of infections.

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Thank you for your attention !

To know more about our research on cyber risk, visit the web site of the Joint Research Initiative

https://sites.google.com/view/cyber-actuarial/home?authuser=0

SORBONNE UNIVERSITÉ
CRÉATEURS DE FUTURS DEPUIS 1257

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling