Propagation of cyber incidents in an insurance portfolio

Caroline Hillairet[1], Olivier Lopez[2]
Joint Research Initiative "Cyber risk: actuarial modeling"
supported by Risk Fundation, AXA Research Fund

[1] **Ensae Paris**, [2] Sorbonne Université

OWARS Seminar, 15th September 2021

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Outline

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.
- Huge costs : estimated to 1% of the global GDP.
- In France, numbers of ransomwares reported to ANSSI multiplied by 3 between 2019 and 2020.

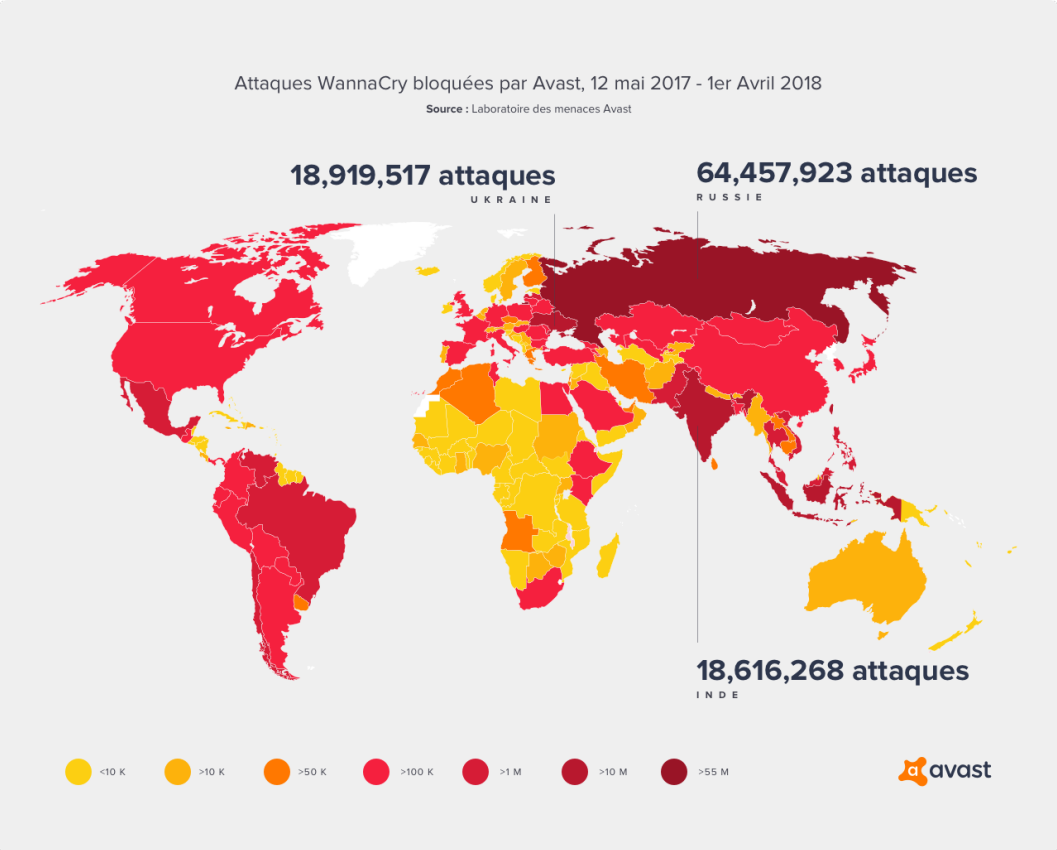
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

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).

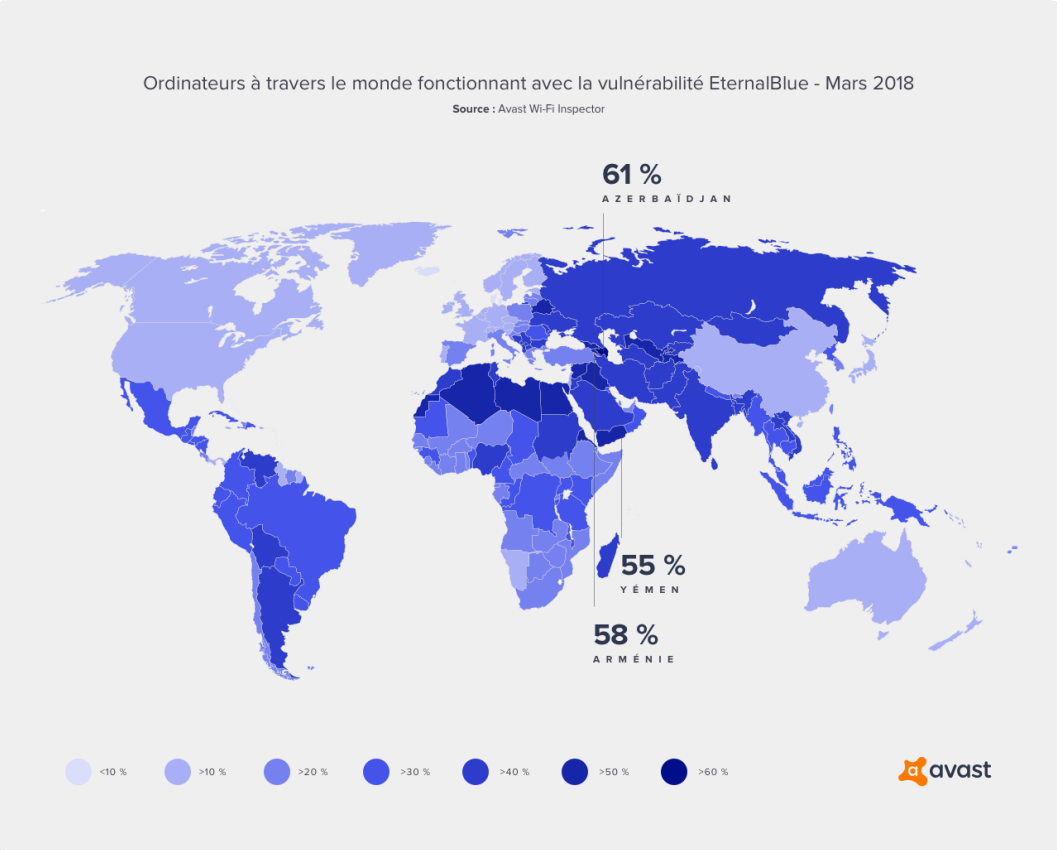
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Wannacry in maps



RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Wannacry in maps



RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

NotPetya

Le Point Tech & Net

Actualité > Tech & Net

Cyberattaque mondiale NotPetya: Londres et Washington accusent la Russie

AFP

Modifié le 15/02/2018 à 23:49 - Publié le 15/02/2018 à 13:07 | AFP

- June 2017. Uses the same vulnerability EternalBlue.
- Strikes mostly Ukraine, but also Saint Gobain ($384 millions losses), Auchan and SNCF.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Cyber insurance products

- Typically, there are four dimensions:
  - financial reparation
  - immediate assistance to restart the activity
  - protection against regulation issues caused by leaks of data
  - crisis communication
- And a fifth dimension, essentially for SME: prevention and risk analysis.

Cyber-risk specificities

- Similarities with operational risk...
- ... but specificities in the structure of cyber events.

1. The risk is new and evolves fast.
2. "Silent cyber": non-cyber policies may content guarantees that can be triggered by cyber events if not excluded.
3. Accumulation risk : potential concentration of incidents which leads to loss of mutualization.
4. Specificity of the repair needed after a cyber event.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Loss of mutualization : when there is no independence

- Example in insurance : natural catastrophes and portfolios with spatial correlations:

- Cyber risk: how to define proximity?

Outline

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).

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

The general model

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

Micro modeling of the cyber-epidemic

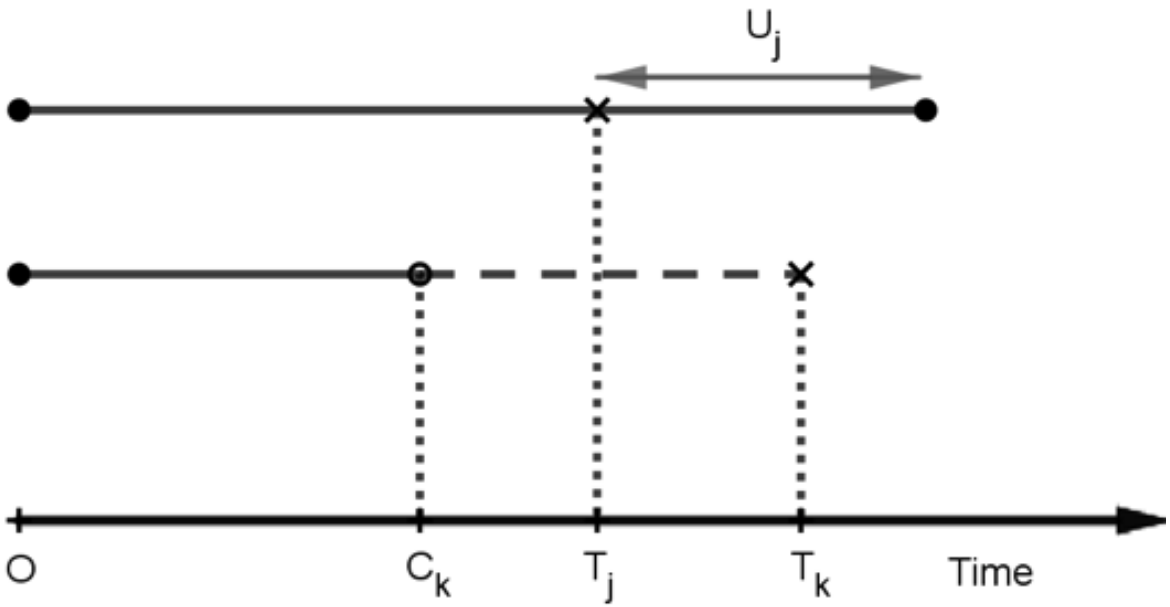
For a policyholder, we define

- 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.

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.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Impact on the portfolio

- Policyholders assumed to be i.i.d., characterized by $(T_i, U_i, C_i)_{1 \leq i \leq n}$.
- We define $\delta_i := 1_{T_i \leq C_i}$.
- Different counting processes

$$\begin{aligned}
\mathfrak{N}_t &= \sum_{i=1}^{n} \delta_i 1_{T_i \leq t} && : \text{cumulative number of infected} \\
\mathfrak{R}_t &= \sum_{i=1}^{n} \delta_i 1_{T_i + U_i \leq t} && : \text{number of recovered} \\
\mathfrak{I}_t &= \mathfrak{N}_t - \mathfrak{R}_t && : \text{number of currently infected}
\end{aligned}$$

- Different quantities of interest :

$$\sup_{t \geq 0} \mathfrak{I}_t, \text{ or } \int_0^\infty \mathfrak{I}_t dt = \sum_{i=1}^{n} \delta_i U_i.$$

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Hazard rate function

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

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

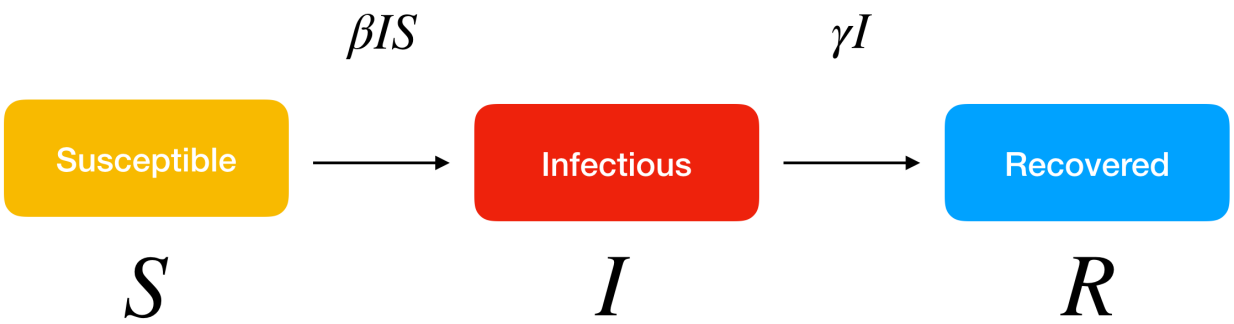
- Link with the density function f_T and the survival function $S_T = \mathbb{P}(T \geq t)$:

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

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

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

SIR model Flow Chart



- β : Infection rate
- γ : Recovery rate
- $\mathcal{R}_0 = N\beta/\gamma$: Basic reproduction number.
  If $\mathcal{R}_0 > 1$, an epidemic appears, otherwise it vanishes.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

SIR model

- SIR model : prey-predators model. Define:
  - $S(t) =$ "Susceptible" (those who are exposed in the global population);
  - $I(t) =$ "Infected" (and contagious);
  - $R(t) =$ "Recovered" or "Removed" (no longer contagious).
- Differential equations system :

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

- Constant size of the population : $N = S(t) + I(t) + R(t)$.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

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 :

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

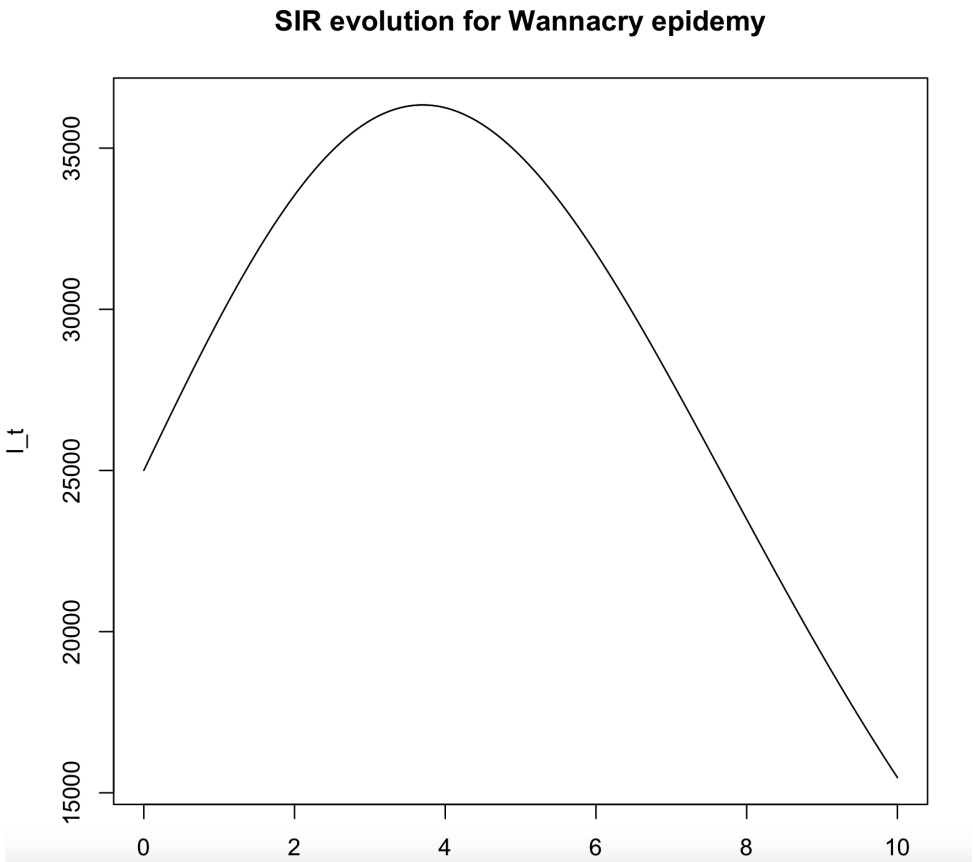
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

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).

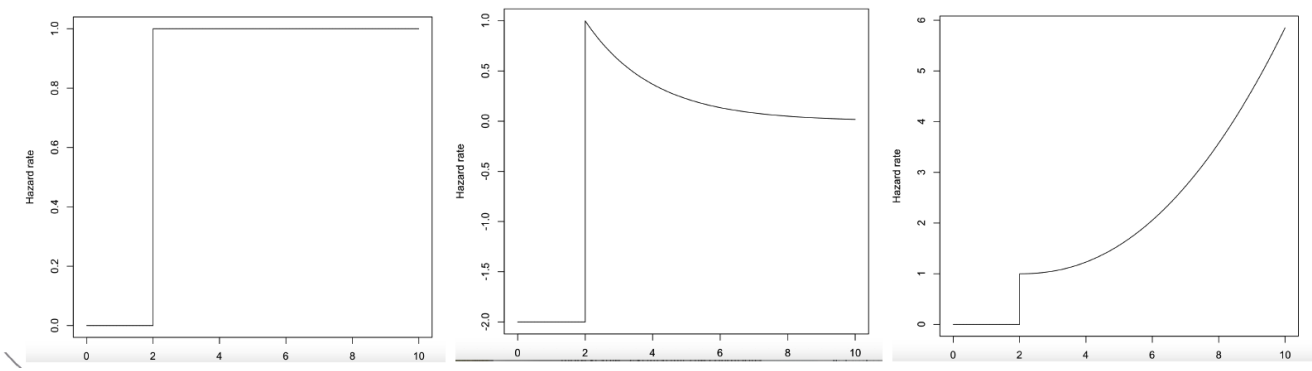
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Example of epidemic dynamics of Wannacry type



Reaction

- Three examples of behavior (hazard rate) :



- From left to right "Exponential", "Pareto", "Weibull".
- In the three cases, three reaction delays, and different hazard rates.

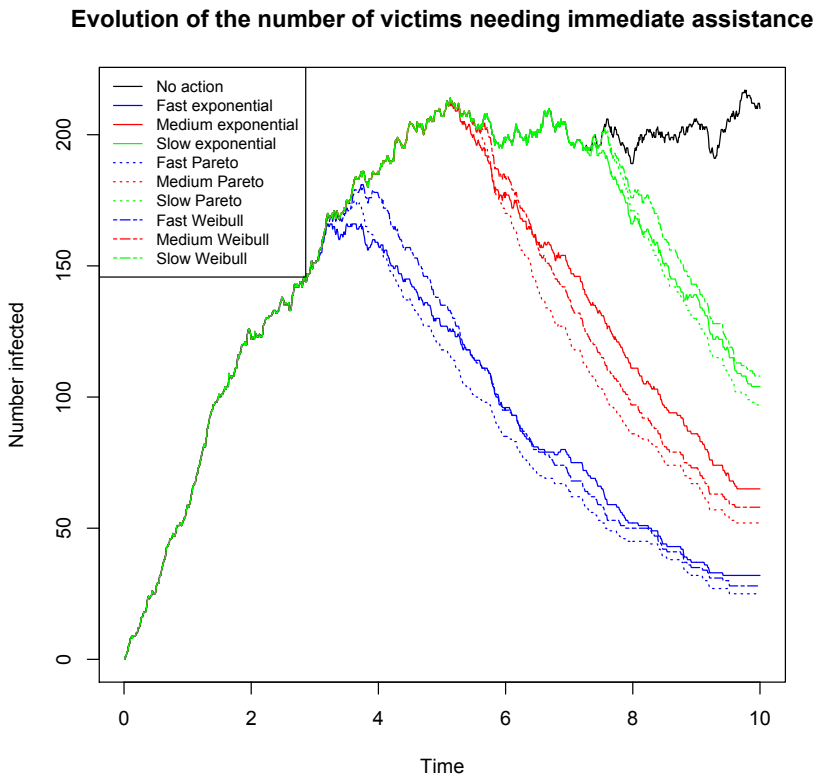
What can we quantify with this model ?

- 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.
- Saturation : if a large number of policyholders are simultaneously victims of the attack, the insurer may not be able to assist them all (causing then an increase of the costs).

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Simulation of a Wannacry-type scenario

- Simulation on a portfolio of 10 000 policyholders.



RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Simulation results

- In this example, we see that the speed of reaction is crucial to reduce the peak.
- A late intervention still reduces the final number of policyholder infected.
- Regarding the way the three behaviors affect the peak: mixed picture.
- In Hillairet and Lopez (2021): if one assumes a shape on the cost of intervention (which may be dependent on the current number of policyholders needing assistance), one can determine the cost of concluding a partnership with a certain capacity of response.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Outline

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Multi-group SIR models

- Aim:Take into account connexions between members of different types on the portfolio that can contaminate themselves.
- 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.

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 $\alpha_i(t) = \alpha 1_{0 \le t < 1}$ for some i.

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: $\eta_i(t) = \eta 1_{S_i(0)/S_i(t)\geq s}$.

Final number of victims

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

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

where

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

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

- From R, one deduces the probability of being hit for each category present in the portfolio.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

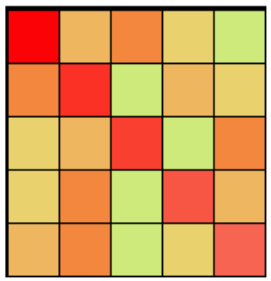
Impact of the connectivity

- 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.

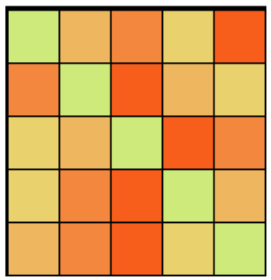
RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Two examples of matrices

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



- Non-clustered:



RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

Comparison with a reference scenario

- Reference scenario: one single class, infection similar to Wannacry, initialization through an attack function $\alpha_1(t) = \alpha_0 1_{0 \leq t \leq 1}$.
- 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

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*.
- -> 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.

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling

References

- On contagion scenarii:

  Hillairet C., Lopez O. (2021) **Propagation of cyber incidents in an insurance portfolio: counting processes combined with compartmental epidemiological models**, in *Scandinavian Actuarial Journal* https://www.tandfonline.com/doi/abs/10.1080/03461238.2021.1872694.
- Preprint: https://hal.archives-ouvertes.fr/hal-02564462/
- Joint Research Initiative "Cyber-insurance: actuarial modeling" : https://sites.google.com/view/cyber-actuarial/home?authuser=0

RESEARCH INITIATIVE
Cyber Risk: Actuarial Modeling