OPINIONS
& DÉBATS

N°24 - Janvier 2022

Cyber-assurance : enjeux, modélisations et leviers de mutualisation

Cyber insurance: issues, modelling and mutualisation levers

Caroline Hillairet & Olivier Lopez

INVESTIR L'AVENIR

LABEX Louis Bachelier

SOMMAIRE

Opinions & Débats N° 24 - Janvier 2022

Publication de l'Institut Louis Bachelier

Palais Brongniart - 28 place de la Bourse 75002 Paris ◆ Tél. : 01 73 01 93 40 ◆ www.institutlouisbachelier.org

DIRECTEUR DE LA PUBLICATION : Jean-Michel Beacco ◆ **COORDINATION ÉDITORIALE** : Ryadh Benlahrech

CONTACT : ryadh.benlahrech@institutlouisbachelier.org

CONCEPTION GRAPHIQUE : Vega Conseil 01 48 85 92 01

CONTENTS

Les articles publiés dans la série “Opinions & Débats”offrent aux spécialistes, aux universitaires et aux décideurs économiques un accès aux travaux de recherche les plus récents. Ils abordent les principales questions d’actualité économique et financière et fournissent des recommandations en termes de politiques publiques.

The Opinions and Debates series sheds scientific light on current topics in economics and finance. Bringing together several types of expertise (from mathematicians, statisticians, economists, lawyers, etc.) this publication makes recommendations in the formulation and implementation of public economic policy.

EDITO

Jean-Michel Beacco
Délégué général
de l'Institut Louis Bachelier

Avec la transformation digitale à l'œuvre depuis plusieurs années, les risques cyber sont devenus une menace grandissante pour beaucoup d'entreprises, en particulier les PME et les ETI. Ces dernières disposent rarement des ressources humaines internes pour faire face à des attaques cyber, et ne possède aucune couverture assurantielle pour couvrir ce type de risque. En outre, l'essor du télétravail, en raison de la pandémie, a accentué la vulnérabilité des entreprises à ces attaques.

Du côté des assureurs, la forte sinistralité enregistrée sur les risques cyber affecte déjà leur rentabilité : le volume des primes a bondi de 49 % et le ratio des sinistres sur primes a atteint 167 % en 2020, contre 84 % l'année précédente. Les chiffres de l'année 2021, encore non disponibles, ont très certainement poursuivi leur hausse, du moins concernant le nombre d'attaques cyber. Résultat ? Les primes d'assurance pour couvrir les risques cyber explosent à la hausse, parallèlement aux niveaux de couverture qui eux sont revus à la baisse, selon des courtiers spécialisés. Cette situation menace à la fois les entreprises peu ou pas couvertes, mais aussi le secteur assurantiel en cas de contagion simultanée à des milliers de clients, jusqu'à mettre en péril le principe de mutualisation sur lequel est fondé l'assurance.

Ces problématiques sont urgentes à résoudre, d'autant plus qu'elles risquent de croître dans les années à venir, parallèlement à la transition numérique. À l'Institut Louis Bachelier, le programme de recherche *Cyber Insurance risk: actuarial modeling*, dirigé par Caroline Hillairet et Olivier Lopez, est actif depuis plus de trois ans pour produire des travaux académiques permettant d'orienter les acteurs du secteur.

Vous trouverez une illustration de ces travaux de recherche dans ce nouveau numéro de la collection *Opinions & Débats*. Caroline et Olivier reviennent sur les grandes inquiétudes liées aux risques cyber et émettent des recommandations pour que ces risques soient mieux mutualisés au sein du secteur assurantiel qui, après les victimes, est en première ligne face à ces menaces.

Bonne lecture et bonne année 2022 à tous les lecteurs d'*Opinions & Débats* !

With the digital transformation that has been underway in recent years, cyber risks have become a growing threat for many companies, especially SMEs and SMIs. These businesses rarely have the internal human resources to deal with cyber attacks, and have no insurance coverage for this type of risk. In addition, the rise of working from home due to the pandemic has increased companies' vulnerability to these attacks.

For insurers, the high level of claims arising from cyber risks is already affecting their profitability: premium volume jumped by 49% and the loss ratio rose to 167% in 2020, compared to 84% the previous year. The figures for 2021, which are not yet available, have certainly continued to rise, at least in terms of the number of cyber attacks. As a result, Insurance premiums to cover cyber risks are skyrocketing, while coverage levels are being reduced, specialized brokers say. This situation threatens not only businesses with little or no coverage, but also the insurance sector in the event of simultaneous contagion to thousands of customers, to the point of jeopardizing the principle of mutualisation on which insurance is based.

These problems need to be resolved as a matter of urgency, especially as they are likely to increase in the coming years, in parallel with the digital transition. At the Institut Louis Bachelier, the Cyber Insurance risk: actuarial modeling research programme, directed by Caroline Hillairet and Olivier Lopez, has for more than three years been actively producing academic work to guide actors in the sector.

You will find an example of the research work in this new issue of the *Opinions & Débats* series. Caroline and Olivier discuss the major concerns related to cyber risks and make recommendations for their better mutualisation in the insurance sector, which, next to the victims themselves, is in the front line in the face of these threats.

Enjoy your reading and Happy New Year 2022 to all readers of *Opinions & Débats*!

Jean-Michel Beacco
Delegate General of the Institut Louis Bachelier

BIOGRAPHIE

Caroline Hillairet

Caroline Hillairet est Professeure à ENSAE Paris et responsable de la formation actuariat depuis 2015. Elle est membre du CREST (Centre de Recherche en Economie et Statistique), laboratoire de finance et assurance. Elle est membre du conseil d'administration de l'Institut des actuaires depuis 2020. Elle est co-directrice, avec Olivier Lopez, de l'Initiative de Recherche de la Fondation du Risque, sur l'évaluation actuarielle du risque cyber.

Caroline Hillairet has been a Professor at ENSAE Paris since September 2015, in charge of the actuarial programme. She is a member of the Center for Research in Economics and Statistics (CREST) and the LFA (Finance and actuarial science) laboratory. She is board member of the French Institute of Actuaries since 2020. She is co-director, with Olivier Lopez, of the Research Initiative of the Risk Foundation, on the actuarial modeling of cyber risk.

Olivier Lopez est Professeur à Sorbonne Université en mathématiques appliquées, directeur de l'ISUP (Institut de Statistique) depuis 2016. Membre agrégé de l'Institut des actuaires, ses travaux de recherche portent sur les méthodes statistiques de quantification des risques, notamment en assurance. Il est co-porteur, depuis 2018, d'une initiative de recherche de la Fondation du Risque sur la modélisation en cyber-assurance. Il est également l'un des directeurs scientifiques de Detralytics depuis 2021.

Olivier Lopez

Olivier Lopez is Professor in applied mathematics at Sorbonne Université and has been director its Institute of Statistics (ISUP) since 2016. A fully qualified member of the French Institute of Actuaries, in his research he focuses on the use of statistical methodology to quantify risk, especially in insurance. Since 2018 he has been co-chair of a Risk Foundation research project on actuarial models for cyber insurance. He was appointed scientific director of Detralytics in 2021.

Cyber-assurance : enjeux, modélisations et leviers de mutualisation

Caroline Hillairet
ENSAE Paris, Centre de Recherche en Économie et Statistique

Olivier Lopez
Sorbonne Université, ISUP, Laboratoire de Probabilités, Statistique et Modélisation

Résumé

La croissance de l'économie digitale a apporté de profondes transformations dans la plupart des secteurs économiques. Ces mutations ont modifié la cartographie des risques encourus par les entreprises, notamment les risques liés aux systèmes d'information. En quelques années, le cyber-risque est apparu comme l'une des menaces principales pesant sur les entreprises, comme l'indique notamment le rapport du Ministère de l'Intérieur [RM19] sur le sujet. L'assurance apparaît dès lors comme un outil favorisant la résilience de l'économie face à ce risque majeur, voire un élément de cyber-défense. Mais si le marché de la cyber-assurance se développe - en mettant en avant des offres innovantes qui couplent prévention, réparation financière, et accompagnement en cas de crise - de nombreuses questions se posent sur leur viabilité, et sur la capacité du secteur à mutualiser les pertes en cas de sinistre majeur. Dans cet article, nous discutons les problématiques techniques posées par la quantification du risque cyber. Nous expliquons en quoi des modélisations mathématiques adaptées peuvent contribuer à une meilleure évaluation du risque et à la viabilité du modèle économique de l'assurance cyber. La pertinence de ces modèles est actuellement limitée par la faiblesse des données disponibles. Nous émettons des recommandations pour un partage d'information entre acteurs, élément essentiel à la résilience de nos sociétés face à la menace cyber.

I. Introduction

Avec la croissance de l'économie digitale, le risque cyber est devenu l'une des menaces principales pesant sur les entreprises (cf. notamment le rapport 2019 du Ministère de l'Intérieur [RM19]). Pour Jerome Powell, président de la Réserve Fédérale américaine, les cyber-attaques constituent aujourd'hui la principale menace pesant sur le système financier mondial. Cette menace est amplifiée depuis la crise sanitaire liée à la pandémie de Covid-19, comme le pointe le rapport d'activité pour l'année 2020 de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) [ANSSI21a] : ce rapport conclut sur une explosion des cyber-attaques, en particulier des rançongiciels, dont les signalements ont plus que triplé entre 2019 et 2020.

Face au cyber-risque, l'assurance a un rôle crucial à jouer en termes de réparation notamment financière. La cyber-sécurité physique, essentielle pour limiter et prévenir les attaques, ne peut en effet parvenir à constituer un bouclier impénétrable contre ces agressions numériques. Mais pour voir émerger une protection financière économiquement viable, il est nécessaire de quantifier les impacts de ce risque. Or cette évaluation d'un risque aux multiples facettes nécessite des techniques statistiques et probabilistes avancées en vue d'anticiper les coûts, l'évolution de la menace et de ses impacts financiers, afin de surmonter les défis inhérents à la cyber-assurance.

En vue de mieux saisir ces enjeux, décrivons tout d'abord la nature même du risque à travers quelques exemples d'événements cyber marquants, avant de présenter quelques éléments descriptifs du marché actuel de l'assurance cyber.

1.1. Descriptif et exemples d'attaques cyber

Les attaques cyber sont un phénomène aussi ancien que l'informatique. Néanmoins, la dépendance accrue des économies au digital, ainsi que l'intensification de la connectivité des agents économiques, ont changé la nature et l'impact de ces événements. Les attaques Wannacry (voir [MP17] et Encadré 1) et NotPetya (voir [T17] et [F18]) sont espacées de quelques semaines et sont deux exemples marquants d'attaques massives. Elles frappent, en l'espace de quelques jours, environ 300 000 machines dans 150 pays pour Wannacry, et des millions dans 65 pays pour NotPetya. Les pertes causées sont considérables, même si elles sont difficiles à quantifier avec précision. Les estimations vont de plusieurs centaines de millions à 4 milliards de dollars pour Wannacry, voir [EUROPOL18], et à plus de 10 milliards de dollars pour NotPetya, voir [B20] et [CISA20]. Ce chiffrage difficile est notamment lié au fait que les consequences indirectes qu'ont pu subir les victimes peuvent être parfois plus importantes que les dommages immédiats. D'après Bruno Charrat, copilote du programme Cybersécurité du CEA, "1 % du PIB mondial, soit 1 000 milliards de dollars, partirait chaque année en fumée à cause de la cybercriminalité." (Cf. [CEA21]).

Ces deux attaques emblématiques, Wannacry et NotPetya, appartiennent à la classe des attaques par rançongiciel. Ces logiciels malveillants infectent un système d'information en exploitant une faille de celui-ci, aussi appelée vulnérabilité. Parfois, il s'agit de nouvelles vulnérabilités : on parle alors de "*Zero Day Exploit*", où la faille, tout juste découverte par les hackers, surprend les acteurs de la cyber-sécurité. Mais le plus souvent, ce sont des vulnérabilités bien identifiées qui sont exploitées, et pour lesquelles des correctifs existent.

C'est le cas de la vulnérabilité *Eternal Blue* (voir [T17]) utilisée par Wannacry et NotPetya, qui aurait pu être colmatée par simple mise à jour des systèmes en amont de la crise. Une fois introduit via la faille, le virus bloque l'accès aux informations contenues dans le système et cet accès n'est restitué qu'une fois la rançon payée[1].

Comme nous l'avons déjà indiqué, les dommages liés à ces attaques ne sont en général pas seulement liés aux rançons. Dans le cas de Wannacry, le montant des rançons est connu, car les transactions sur les adresses bitcoin sont publiques à défaut de pouvoir tracer leur destination. Néanmoins, le coût de ces rançons est très faible au regard de la perte totale. Celle-ci est notamment causée par la perte d'exploitation, comme dans le cas de l'attaque contre Colonial Pipeline (voir [E21]), ou encore par les risques légaux et de réputation. C'est le cas notamment lorsqu'on se trouve confronté à une attaque à "double extorsion" : le blocage des données est précédé par une exfiltration de celles-ci, avec la menace de leur divulgation. Si des données personnelles sont touchées, cet événement peut tomber sous le coup du Règlement Général sur la Protection des Données (RGPD). Par ailleurs, des informations confidentielles ou des secrets industriels peuvent être dévoilés.

À cette variété de dommages causés par le cyber, s'ajoute la variété des cibles (entreprises, états, collectivités publiques, particuliers…) et des types d'attaques. Outre les rançongiciels (dont l'utilisation connaît de nombreuses variantes), les attaques par déni de service (Ddos) consistent à saturer de demandes un serveur, entraînant sa mise hors service. Les motivations des hackers, et donc les dommages qu'ils causent, sont là aussi très variés, allant du simple acte criminel visant l'enrichissement personnel, à des actions étatiques, en passant par des actes militants ("hacktivism").

1.2. Marché de l'assurance cyber

Les polices d'assurance cyber ont commencé à être proposées dans les années 1990, sous forme de packages (logiciel + assurance), par des éditeurs de logiciels de sécurité en partenariat avec des sociétés d'assurance (cf. [BM09]). Au fil des années, le marché de la cyber-assurance "*stand-alone*" (polices dédiées uniquement au risque-cyber) s'est développé, principalement aux États-Unis, avec des clauses spécifiques, afin de s'adapter à l'évolution continue des cyber-attaques et à la complexité des systèmes d'information. Les réglementations sur la protection des données (la première étant la loi sur la notification des violations de données adoptée en Californie en 2003) ont également été un moteur important du marché de la cyber-assurance. Plusieurs études qualitatives sur les polices d'assurance cyber, principalement américaines, ont été publiées, comme celle de [MMN+15] qui comparent notamment les couvertures de plusieurs polices d'assurance. Plus récemment, [RAK+19] dressent un panorama du marché de l'assurance cyber aux États-Unis (plus précisément les états de New-York, Pennsylvanie et Californie) concernant les pertes couvertes dans les polices d'assurance, les questionnaires renseignés lors de la souscription, ainsi que les facteurs entrant dans le calcul des primes d'assurance. Même si l'exemple du marché de la cyber-assurance aux États-Unis est porteur de leçons car plus mature, il ne se transpose pas totalement au cadre spécifique du marché français et plus généralement européen, notamment concernant l'importance des cas de fuite de données personnelles.

1. Cette restitution n'est pas automatique. Ainsi, dans le cas de Wannacry, les paiements ne permettaient pas de débloquer le système d'information, voir [MP17]. Plus récemment, Colonial Pipeline, malgré le versement d'une rançon de 4 millions de dollars, n'a pas retrouvé toutes ses données, voir [E21].

Face à ce risque aux multiples facettes, les assurances cyber en Europe incluent également des garanties variées, typiquement :

- Garantie réparation des dommages et rétablissement du système d'informations.
- Garantie pertes d'exploitation en cas d'interruption d'activité.
- Garantie responsabilité civile, en cas de fuites de données personnelles, pour se conformer à la réglementation européenne RGPD (potentiels frais juridiques et amendes).
- Garantie sur les frais de communication en cas de crise, car un incident cyber peut ternir l'image de l'entreprise.

Néanmoins, malgré ces multiples garanties, les dommages réels ne sont pas toujours inclus ou anticipés dans les garanties des assurances cyber, et peuvent être dramatiques : citons le décès d'une patiente en 2020 à la suite de la cyberattaque de l'hôpital universitaire de Düsseldorf en Allemagne, même si les investigations ont requalifié l'événement en "perte de chance" et non en homicide. Par ailleurs, une attaque cyber peut déclencher des garanties de polices d'assurance non-cyber, par exemple un incendie ou bien une explosion, comme ce fut le cas en 1982 après le piratage des systèmes de contrôle d'un gazoduc sibérien.

Les contrats cyber incluent généralement, en plus de la réparation financière, des offres de prévention ainsi que d'assistance en cas de sinistre. Ce volet prévention/assistance est particulièrement utile notamment pour les PME, qui ne possèdent pas toujours l'expertise suffisante face au risque cyber. N'étant qu'observateurs indirects de ces événements, le rôle des assureurs au moment d'une attaque est souvent limité par rapport aux sociétés de cyber-sécurité ou à l'État. Ils peuvent, néanmoins, constituer un relai précieux d'information contribuant à réduire des menaces plus permanentes. Par ailleurs, grâce notamment aux questionnaires à renseigner lors de la souscription et au conditionnement du tarif, l'assureur est un acteur clé pour une meilleure connaissance du risque de la part de l'assuré, et pour l'inciter à améliorer son hygiène cyber. Ces questionnaires et audits pourraient également contribuer à réaliser une cartographie du risque, à l'image d'un "zonier" virtuel, pour une meilleure diversification du risque et donc une meilleure assurabilité.

En France, l'étude "Lumière sur la Cyber-Assurance" (LUCY) de l'AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise) fournit également une photographie précise des primes perçues en France, ainsi que de la sinistralité sur les années 2019 et 2020. Cette étude [LUCY21], réalisée à partir de données de courtiers, est l'une des rares sources fiables sur le secteur, bien que ne captant pas les sinistres pouvant avoir été subis par des TPE/PME ou ETI.

Si le développement du marché est en cours et répond à un besoin croissant, il achoppe sur un certain nombre de difficultés, ce qui peut expliquer le ralentissement en France des souscriptions après un développement important : d'après les enquêtes annuelles OpinionWay pour le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) [CESIN], 19 % des répondants avaient souscrit une assurance cyber en 2015, contre 50 % en 2019 et 60 % en 2020. Alors qu'aujourd'hui 87 % des grandes entreprises sont couvertes par un contrat d'assurance cyber, le taux de couverture des TPE/PME, ETI et collectivités publiques est encore largement insuffisant (seul 8 % pour les ETI, d'après [LUCY21]). Or ces entreprises sont particulièrement vulnérables contre le risque cyber, à la fois en termes de capacités à analyser leur propre risque, à cerner et mettre en œuvre les bonnes pratiques de sécurité informatique, tant qu'en termes de matelas financier pour amortir les chocs d'une attaque cyber.

L'une des difficultés rencontrées par les assureurs tient dans la nécessité de redéfinir le périmètre des contrats, et notamment d'identifier, dans des polices non-cyber (par exemple des polices responsabilité civile), les cas où un incident cyber pourrait activer la garantie. Cette situation - on parle de couverture silencieuse, ou "silent cyber" - pourrait en effet déséquilibrer des portefeuilles existants, dont l'équilibre n'est pas pensé pour supporter les conséquences importantes d'un sinistre de cette nature. Le travail d'identification des couvertures silencieuses s'accompagne donc de la construction de couvertures dites "affirmatives" qui trouvent leur place dans des contrats d'assurance cyber dédiés.

Mais les enjeux de l'éclosion du marché cyber ne sont pas limités à cette problématique de formulation ou d'exclusion de certains faits générateurs. L'étude LUCY de l'AMRAE attire notre attention sur les S/P (rapports "Sinistres sur Primes") extrêmement dégradés sur les années 2019 et surtout 2020 (84 % et 167 % respectivement). Ce ratio S/P rapporte le montant payé au titre des sinistres (S) par les primes reçues pour les absorber (P). Dans un système équilibré, les primes permettent l'absorption du coût des sinistres et un S/P faible traduit une bonne anticipation de l'évolution du risque. Les chiffres extrêmement élevés de l'AMRAE soulignent le flou dans lequel baigne le secteur, et combien la quantification du risque est compliquée.

Dans cet article, nous analysons les raisons qui font du cyber-risque, et de son impact financier, une matière difficile à appréhender. Nous fournissons également quelques pistes qui permettraient, à notre sens, d'aborder ces questions sous un jour prometteur. Dans une première partie, nous rattachons ce risque à la catégorie des risques extrêmes, dont l'étude tombe dans le champ de la théorie statistique des valeurs extrêmes. Ces risques sont caractérisés par une très forte volatilité du coût de chaque événement.

Mais cette sévérité extrême d'un événement frappant une seule victime ne doit pas occulter le danger posé par le caractère systémique de ce risque, que nous évoquons dans une deuxième partie. Par sa capacité à se propager à la vitesse de la fibre optique dans les réseaux de communications, l'attaque cyber peut entraîner des contagions et des défaillances massives pouvant mettre à l'arrêt une économie, ou a minima mettre en danger la solvabilité d'un assureur. Au-delà du diagnostic, nous expliquons quels modèles récents peuvent être utilisés, afin d'anticiper les contre-mesures et leurs impacts face à cette menace.

Ces modèles, indispensables à la quantification du risque, nous amènent à nous interroger sur les données nécessaires pour les calibrer, ainsi que sur les méthodes à mettre en œuvre pour effectuer un suivi adapté à ce risque changeant. Nous envisageons cette question dans une dernière partie, qui traite de recommandations sur la constitution de bases d'informations cohérentes sur le risque, et sur la nécessité d'appréhender les aspects comportementaux, notamment liés à l'écosystème malveillant à l'œuvre derrière les attaques.

Encadré 1 : Un exemple de cyber-attaque massive : le rançongiciel Wannacry

L'accès aux informations contenues dans le serveur infecté par le rançongiciel est bloquée et cet écran apparaît, demandant de payer une rançon pour récupérer les données. Ce virus, exploitant la faille *EternalBlue*, se répand rapidement par Internet et en une semaine, il affecte entre 200 et 300 000 victimes dans 150 pays. Les victimes sont des particuliers, des entreprises de toutes tailles, et des services de santé comme le *National Health Service* (NHS). Les dommages sont considérables : ils sont de l'ordre du milliard de dollars, 92 millions de livres rien que pour le NHS. Ce n'est pas tant le coût de la rançon en elle-même (entre 300 et 600 dollars), mais les nombreuses pertes induites, notamment les pertes d'exploitation, qui sont les plus coûteuses.

II. Risques extrêmes

Le mécanisme de mutualisation découle de la loi des grands nombres (cf. Encadré 2). Or celle-ci suppose l'existence d'une espérance pour la variable aléatoire représentant la perte d'un assuré. Cette existence n'est pas automatique, cette quantité pouvant être infinie pour certaines variables dites à "queue lourde", c'est-à-dire pouvant prendre des valeurs importantes avec une probabilité non négligeable. C'est le cas par exemple des lois de Pareto d'indice de Pareto γ (aussi appelé indice de queue) plus petit que 1 (cf. Encadré 3 et Figure 3).

Ceci semble paradoxal pour des phénomènes réels : une perte est toujours bornée, même si cette borne peut être extrêmement élevée. En particulier, dans le domaine de la cyber assurance, des limites d'indemnisation sont régulièrement introduites. Rappelons d'une part que la question n'est pas seulement d'avoir une espérance finie. Pour pouvoir assurer un risque, il faut que le tarif soit suffisamment attractif et donc faible. Si l'espérance est trop élevée, le modèle assurantiel n'est pas économiquement viable.

Mentionnons également que, dans certaines situations, même si la perte est en théorie bornée, il peut y avoir une très faible différence statistique entre la distribution réelle des pertes et des distributions à queues lourdes utilisées en théorie des valeurs extrêmes (voir par exemple [ABT17]). Ce genre de phénomène se retrouve à travers les données de sinistralité cyber collectées par l'AMRAE dans le cadre de son étude "Lumière sur la cyber-assurance" (voir référence [LUCY21]). Les Figures 1 et 2 montrent une très forte disparité entre les sinistres, un faible nombre d'entre eux étant de montant important par rapport aux cas typiques. Ce type de constat, indiquant une extrême volatilité des coûts, invite à se tourner vers des distributions dites à queues lourdes pour modéliser cette variable.

Le choix d'une distribution de Pareto généralisée n'est pas arbitraire, mais guidé par la Théorie des Valeurs Extrêmes (voir [BGS+06]). Ce champ statistique concerne l'étude et la classification des queues de distributions de phénomènes aléatoires, i.e. les zones de grandes valeurs correspondant à des scénarios pessimistes, mais pas complètement improbables. L'indice de queue ("*tail index*") est la mesure permettant de quantifier la sévérité d'un tel phénomène. Une variable prenant de faibles valeurs aura un indice de queue nul, voire négatif : les lois gaussiennes, très utilisées en probabilité du fait de leur rôle privilégié à travers le Théorème Central Limite (voir Encadré 2), ont ainsi un indice de queue nul. En revanche, les phénomènes particulièrement volatiles seront caractérisés par un indice de queue strictement positif. Dans ce cas, la partie haute de la distribution peut, sous des conditions raisonnables, être approchée par une distribution de Pareto Généralisée.

Dans le cas des données de l'AMRAE, l'ajustement d'une loi de Pareto Généralisée tend à conforter l'hypothèse d'un indice de queue strictement positif dans le cas des coûts des sinistres cyber. Ce type de phénomènes a également été identifié sur des sinistres cyber liés à des fuites de données, voir notamment [MS10] ou [FTL21]. Plus particulièrement, la valeur charnière est 1 : si l'indice de queue dépasse 1, l'espérance est infinie et le risque est "inassurable" sauf à introduire des limites d'indemnisation. Plus on s'approche de 1, plus la situation devient critique, nécessitant un volume d'assurés d'autant plus important pour amortir convenablement le risque.

Face à un tel constat, la solution la plus radicale consiste à exclure le risque : si le risque n'est pas assurable, autant ne pas l'assurer. Sans adopter complètement ce point de vue, redéfinir le périmètre des polices est envisageable, typiquement en introduisant des limites d'indemnisation plus restrictives aux polices.

Cette solution n'en reste pas moins insatisfaisante. D'abord, elle pénalise le client, en réduisant le champ de ses prestations. Elle n'est pas non plus la garantie d'un meilleur résultat pour l'assureur. Celui-ci reste confronté à une forte volatilité du résultat, sauf à imposer des limites ridiculement basses, en décalage avec les attentes des clients. Pour amortir cette volatilité, un nombre important d'assurés devra être atteint. Objectif d'autant plus difficile que les prestations sont peu attractives. Un cercle vicieux s'enclenche.

Figure 1 : Montants des sinistres cyber
(source : étude LUCY de l'AMRAE en 2021)

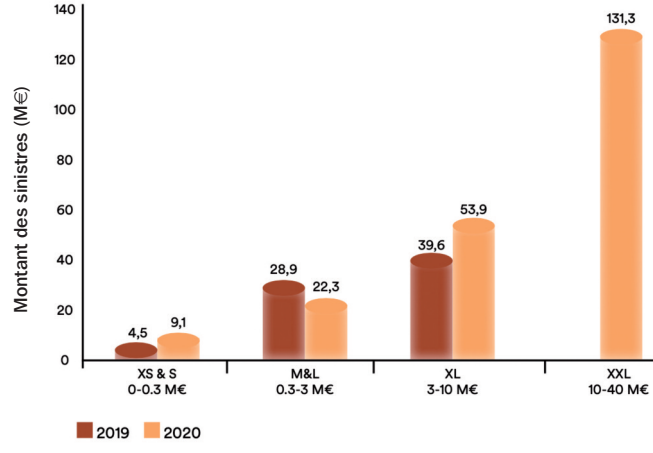
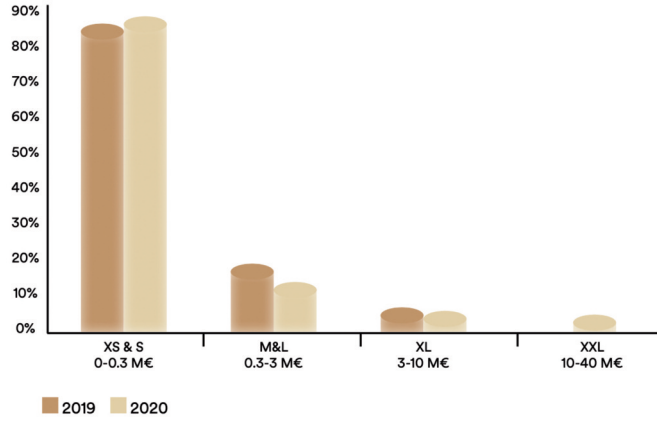


Figure 2 : Proportion de sinistres dans chaque tranche
(source : étude LUCY de l'AMRAE 2021)



Une autre approche consiste à analyser plus finement les causes qui alourdissent la queue de distribution. De façon grossière, notre incapacité à gérer un risque est bien sûr liée à la sévérité de celui-ci, mais est également partiellement liée à notre ignorance. En effet, les sinistres cyber sont de nature extrêmement hétérogène. Aussi bien concernant leur mode opératoire (rançongiciel, attaque par déni de service…), que leurs conséquences (perte d'activité, vol de données personnelles…), ou la nature (secteur médiatiquement exposé ou non…) et le comportement des victimes (négligence, bonne hygiène informatique…). La distribution des pertes est donc la synthèse de cette hétérogénéité.

Le problème, c'est que l'analyse statistique de cet indice de queue, si essentiel dans la compréhension des sinistres sévères, tend à s'aligner sur le pire scénario. Ainsi, prises séparément, deux catégories de sinistres peuvent avoir des indices de queue différents (l'un faible, l'autre proche de 1, qui est la valeur critique). Mises ensemble, sans les distinguer, les méthodes d'estimation statistique s'aligneront sur la queue de distribution la plus lourde, écrasant la partie correspondant à des sinistres de moins grande ampleur, qui pourraient plus facilement être gérés s'ils faisaient l'objet d'un traitement différencié. Cet effet peut être sensiblement atténué par les effectifs dans chacune de ces catégories, mais reste prépondérant sur des volumes de données importants.

Si l'on ne différencie pas l'analyse de ces deux catégories, le danger est alors de pénaliser trop fortement un certain type de sinistres (ou d'assurés). Outre l'insatisfaction compréhensible des clients, une désaffection pour l'assurance peut s'opérer, qui renforce le déséquilibre du système. D'où la nécessité d'analyser finement les facteurs de risque qui pèsent sur la queue de distribution, afin d'opérer une classification efficace des assurés et des types de sinistres. Dans [FTL21], nous proposons des méthodologies combinant *machine learning* et théorie des valeurs extrêmes pouvant être utilisées pour une meilleure classification des événements cyber. Cette méthodologie n'est pas unique, d'autres méthodes, souvent appelées "*tail index regression*", ont été proposées dans la littérature (voir par exemple [BGS+06]) avec chacune leurs avantages et leurs inconvénients.

Dans tous les cas, ces méthodes d'analyse sont prometteuses car elles permettent d'identifier les cas de figure les plus sensibles. À partir de cette compréhension du risque, des stratégies d'optimisation du périmètre du contrat d'assurance sont possibles : par exemple, rendre plus attractives les prestations des risques modérés, afin d'accroître le volume du portefeuille et donc la mutualisation.

La Figure 4 de l'encadré 4 montre ainsi le type de classification qui peut être obtenu à partir de la méthodologie proposée par [FTL21]. Partant d'une population dite "inassurable" (car son indice de queue est supérieur à 1), on parvient, par une étude fine, à observer qu'une large majorité des situations considérées est en fait associée à un indice de queue plus faible que 1 (82 %), quand seule une part réduite (18 %) est inassurable, ou nécessite des contraintes plus importantes pour le devenir.

Pour parvenir à ce degré d'analyse, il est néanmoins indispensable de disposer d'informations suffisantes pour analyser les facteurs de risque les plus déterminants.

Encadré 2 : Mutualisation

La mutualisation est au cœur de l'activité d'assurance. Si l'assureur ne vendait qu'un contrat, l'opération d'assurance se réduirait à un pari, avec en cas de sinistre de l'assuré, une perte potentiellement très importante. L'assureur doit donc essayer de réunir un grand nombre d'assurés homogènes et indépendants pour réaliser une opération de mutualisation : les primes reçues de tous les assurés vont permettre d'indemniser ceux qui auront subi un sinistre.

Ce principe de mutualisation repose sur le théorème mathématique de la Loi (forte) des Grands Nombres (LGN) :

Enoncé LGN : Soit (X_i) une suite de variables aléatoires indépendantes et identiquement distribuées, d'espérance finie notée m. Alors, lorsque n tend vers l'infini, la moyenne empirique $\frac{1}{n}\sum_{i=1}^{n} X_i$ converge (presque sûrement) vers $m = E(X_1)$.

Appliquée dans un contexte d'assurance, la loi des grands nombres signifie que, même si le montant de sinistre X_i (ou indemnité) de chaque assuré i est aléatoire, lorsque les dommages sont distribués de manière identique et indépendante, le montant de sinistre moyen par assuré est en fait presque constant et donc "prévisible", approximativement égale à l'espérance mathématique de l'indemnité. Ceci permet de déterminer une "prime pure" pour le contrat d'assurance.

En outre, plus le nombre d'assurés est grand, plus le coût moyen de l'assurance par individu peut être prévu avec précision. Ceci repose sur le Théorème Central Limite (TCL), qui permet donc de contrôler l'écart entre la charge totale et la prime acquise.

Enoncé TCL : Soit (X_i) une suite de variables aléatoires indépendantes et identiquement distribuées, d'espérance et variance finies notées m et σ^2. Alors lorsque n tend vers l'infini,

$$P(|\sum_{i=1}^{n} X_i - nm| \leq \sigma\sqrt{n}\, q) \to \frac{1}{2\pi}\int_{-q}^{q} \exp(-x^2/2)dx$$

Ainsi, si les risques sont indépendants, identiquement distribués et de variance finie, alors la loi de la charge totale est asymptotiquement gaussienne.

Encadré 3 : Théorie des Valeurs Extrêmes

La Théorie des Valeurs Extrêmes fournit une classification des lois de probabilités en fonction de leur queue de distribution. Elle fournit notamment un cadre théorique qui assure que la queue de distribution (i.e. la loi de probabilité des plus grandes valeurs prises par une variable aléatoire) peut être approchée et extrapolée via une loi simple. Cette extrapolation est particulièrement adaptée aux phénomènes dits “à queue lourde”, tels que ceux rencontrés dans le champ du cyber-risque. Dans cet encadré, nous fournissons quelques éléments d’introduction à ce sujet.

Le théorème de Fisher, Tippett et Gnedenko (voir [BGS+06]) s’intéresse à la loi du maximum d’un échantillon de variables indépendantes identiquement distribuées $(X_1,...,X_n)$. Si l’on note M_n ce maximum, le résultat montre que la distribution de cette quantité (proprement centrée et normalisée) ne peut appartenir qu’à un ensemble restreint de lois de probabilités (GEV, pour *Generalized Extreme Value distribution*). Ces distributions sont celles de variables Z dont la fonction de survie s’exprime comme $H_\gamma(z) = \mathbb{P}(Z \geq z) = \exp(-(1+\gamma z)^{-1/\gamma})$ lorsque $1+\gamma z > 0$ et $\gamma \neq 0$ (ou $H_\gamma(z) = exp(-exp(-z))$ dans le cas $\gamma = 0$).

Le paramètre γ (paramètre de queue de distribution, ou “*tail index*”) devient une façon de caractériser la distribution des plus grandes valeurs prises par les variables X_i : on dit que ces variables sont dans le domaine d’attraction de H_γ.

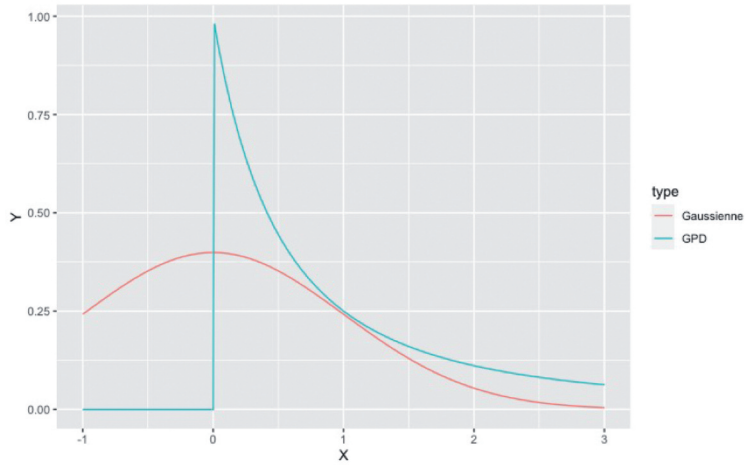
Dans le cas de phénomènes particulièrement volatiles, comme le coût d’un sinistre cyber qui peut prendre des valeurs très éloignées du coût moyen avec une probabilité significative, on se trouve confronté à une valeur de γ strictement positive. Plus γ est important, plus la variable aura tendance à prendre de très grandes valeurs. Ainsi, si $\gamma \geq 1/2$, la notion de variance, traditionnellement utilisée pour quantifier le “chaos” contenu dans un phénomène aléatoire, devient infinie. Si $\gamma > 1$, c’est la notion de valeur moyenne qui est mise en péril, puisque l’espérance de la variable aléatoire devient infinie. Dans ce dernier cas, on parlera parfois d’un risque non-assurable, puisque la tarification repose sur une égalisation de l’espérance des engagements des deux parties (assureur et assuré).

Un théorème de Pickands assure par ailleurs que, si $\gamma > 0$, la distribution de la queue de distribution du phénomène peut être approchée par une loi de Pareto généralisée. Mathématiquement, si l’on introduit $S_u(x) = \mathbb{P}(X - u \geq x | X \geq u)$ c’est-à-dire la fonction de répartition des excès (la loi de $X - u$ conditionnellement au fait que $X \geq u$), on a $\lim_{u\to\infty} \sup_{x>0} |S_u(x) - G_{\gamma,\sigma(u)}(x)| = 0$ pour une certaine fonction $\sigma(u) > 0$ et où

$G_{\gamma,\sigma}(x) = \frac{1}{\left(1+\frac{x\gamma}{\sigma}\right)^{1/\gamma}}$ est la fonction de survie d’une loi de Pareto Généralisée.

Ce résultat est particulièrement intéressant si l’on souhaite modéliser la queue de distribution de la variable aléatoire et notamment anticiper des valeurs particulièrement élevées qu’elle pourrait prendre. D’un point de vue statistique, on essaiera de déterminer parmi les observations un seuil u à partir duquel l’approximation de Pareto généralisée semble raisonnable. Ce choix résulte d’un compromis : u doit, d’une part, être suffisamment grand pour que l’approximation de Pareto généralisée soit légitime. Mais, d’autre part, il doit être suffisamment petit pour qu’un nombre conséquent d’observations de notre échantillon soient au-dessus de ce seuil. Ces observations excédant u vont en effet servir à estimer les paramètres γ et σ , et de leur nombre dépendra la qualité de l’estimation.

Figure 3 : Comparaison graphique d'une densité de probabilité d'une loi gaussienne et d'une loi de Pareto généralisée (GPD)

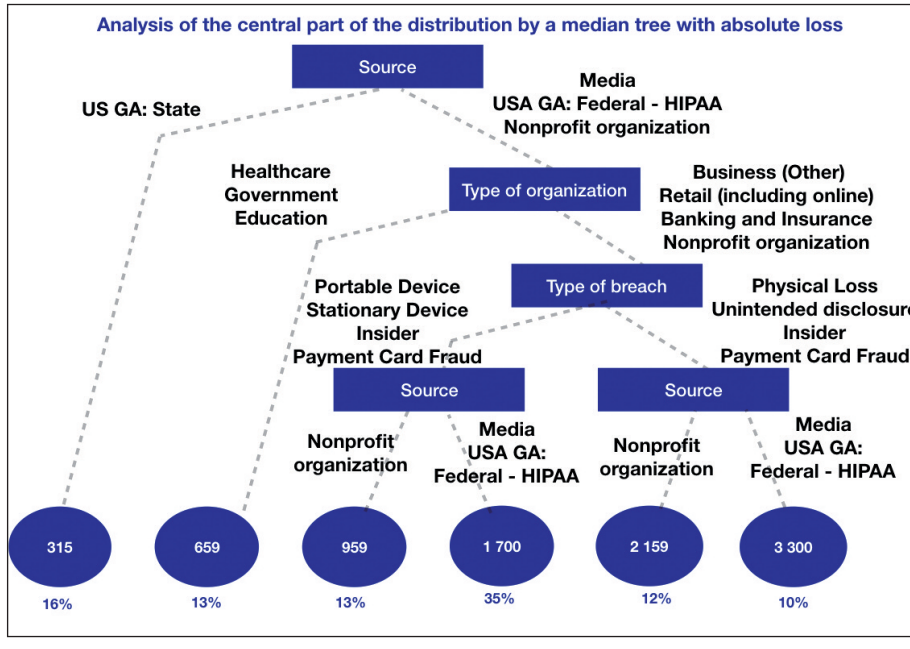


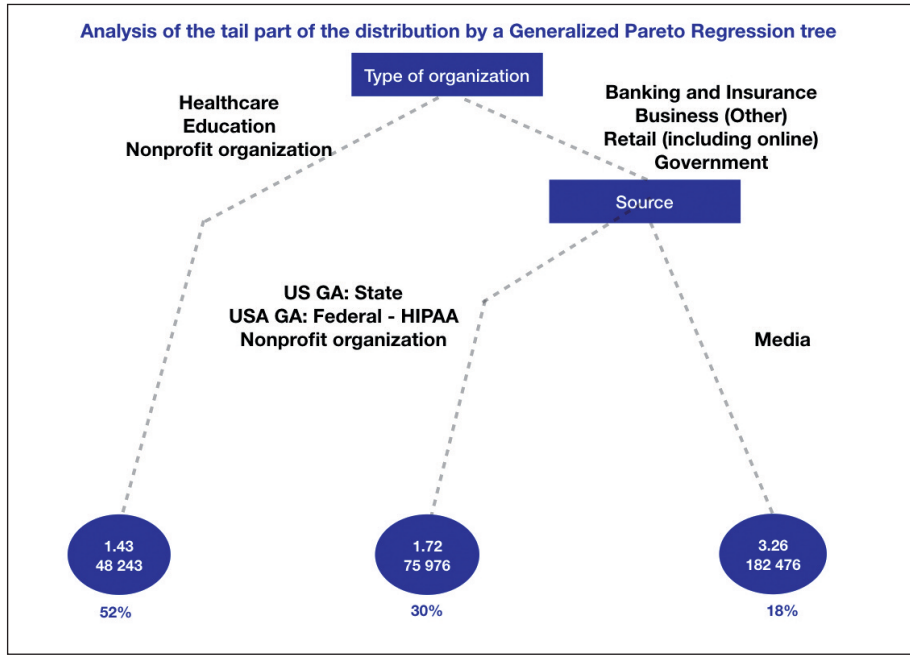
On note la décroissance lente de la densité de la loi de Pareto généralisée, symptôme du caractère explosif de la distribution (de grandes valeurs peuvent être prises avec une probabilité relativement forte).

Encadré 4 : Arbres de classification

La Figure 4 ci-dessous représente deux arbres de régression obtenus par analyse de la base de données PRC (voir Encadré 5) qui recense des fuites de données. Chaque nœud de l'arbre correspond à une variable caractéristique du sinistre, comme le type d'organisation frappée (liste complète des caractéristiques dans [FTL21]). En fonction de la valeur de cette caractéristique, on parcourt la branche gauche ou droite correspondante. Les feuilles de l'arbre (au bas de chaque figure) représentent les classes de risques ainsi obtenues. Le premier arbre correspond à une analyse de la partie centrale de la distribution, c'est-à-dire qu'il met en évidence les facteurs déterminants concernant la sévérité (ici exprimée en volume de données perdues) d'un événement cyber standard. Le second arbre fournit une classification en termes de queue de distribution : chaque feuille de l'arbre représente une classe de sinistres associée à une différente valeur du paramètre γ, premier nombre présent dans la bulle, et σ, second nombre (voir Encadré 3 pour la signification de ces paramètres). [FTL21] notent la disparité géométrique entre ces deux graphes, attestant que les déterminants d'un sinistre typique sont différents de ceux d'un événement sévère. À noter que les auteurs identifient un seuil de γ égal à 2 (portant sur la distribution du volume de données perdues et non sur le montant du sinistre) au-dessus duquel la catégorie d'incidents apparaît comme non assurable. On note sur le second arbre que 82 % des cas correspondent à un γ plus petit que 2, quand seulement 18 % paraissent critiques. Par ailleurs, [FTL21] montrent qu'une analyse de ces données sans faire la distinction entre ces différents types d'événements conduirait à conclure à une inassurabilité globale de ceux-ci.

Figure 4 : Arbres de classification obtenus dans [FTL21] sur les données de la base PRC





III. Composantes systémiques

Parmi les nombreuses caractéristiques des cyber-événements, celles liées au caractère systémique et aux comportements d'auto-excitation sont d'une importance majeure. Cette composante systémique du risque cyber est exacerbée par le fait que la majorité des systèmes d'information présentent les mêmes failles et sont interconnectés.

3.1. Auto-corrélation et clustering d'événements cyber : modélisation par processus de Hawkes multivariés

Dans ce contexte, la modélisation de la fréquence des cyber-attaques nécessite de refléter des effets de dépendance complexes. Or les modèles actuariels standards utilisent le processus de Poisson pour modéliser la composante fréquence du risque. Ce modèle de Poisson repose sur l'hypothèse d'indépendance entre les arrivées de sinistres, et apparaît donc insuffisant pour prendre en compte l'auto-corrélation entre les cyber-événements et les effets de clustering. Ces phénomènes d'auto-corrélation sont illustrés dans la Figure 5, qui représente les auto-corrélogrammes d'événements de failles de données recensés dans la base Privacy Rights Clearinghouse [PRC], cf. Encadré 5.

On constate que les dates d'arrivées d'événements ne sont pas indépendantes (les points ne sont pas uniformément distribués dans les fenêtres), et l'auto-corrélation augmente significativement si on se concentre sur les attaques de type/secteur identiques. Par ailleurs, un test de Kolmogorov-Smirnov (cf. [F62]) rejette l'hypothèse de distribution exponentielle pour les inter-temps, avec une p-valeur proche de zéro[2]. D'où la nécessité d'avoir recours à des modèles dynamiques dont l'intensité d'arrivée des événements (aussi appelée taux de hasard) est stochastique.

L'alternative proposée dans [BBH20] s'appuie sur des modèles de Hawkes multivariés, qui ont la capacité de capter l'auto-excitation et les interactions des cyber-événements en fonction de leurs caractéristiques, tout en bénéficiant d'une représentation paramétrique interprétable et relativement parcimonieuse. Les processus de Hawkes sont des processus de comptage dont l'intensité est entièrement spécifiée par le processus lui-même (cf. Encadré 6 et Figure 6).

Plusieurs fonctions d'excitation ϕ peuvent être utilisées, la fonction exponentielle étant la plus courante (car elle permet des calculs explicites, grâce à la structure markovienne de l'intensité dans ce cadre-là). Mais d'autres noyaux, notamment avec délai, correspondent parfois mieux aux données (comme c'est le cas avec les données PRC, cf. [BBH20]).

Introduits initialement par Hawkes [H71] et utilisés historiquement en sismologie pour modéliser les répliques de tremblement de terre, ils ont été depuis largement utilisés dans de nombreux domaines différents, parmi lesquels la finance, la neurologie, la dynamique des populations ou la modélisation des réseaux sociaux, notamment pour leur capacité à traduire des effets d'excitation. Concernant le cyber-risque, un des premiers travaux est celui de Baldwin et ses coauteurs [BGI+17], qui soulignent la pertinence des processus

[2] Lorsque l'on effectue un test d'hypothèses, celui-ci est basé sur le calcul d'un indicateur à partir de l'échantillon (on parle de statistique de test). La valeur de cette statistique de test est comparée à un seuil qui décide du rejet ou du non-rejet de l'hypothèse par défaut appelée hypothèse nulle. Ce seuil dépend du degré de "prudence" du statisticien (on parle de niveau du test). Une p-value faible (proche de 0) signifie que n'importe quel statisticien utilisant un niveau "raisonnable" rejettera l'hypothèse nulle.

de Hawkes pour modéliser l'occurrence de cyber-attaques dans les systèmes d'information, car ils capturent à la fois les chocs et la persistance après les chocs qui peuvent former une contagion des attaques.

Ce comportement d'auto-excitation entraîne le regroupement (phénomène de clustering) et l'auto-corrélation des arrivées de cyber-événements.

Au vu de l'hétérogénéité du risque cyber, des types d'attaques et de leurs cibles, [BBH20] propose une modélisation via des processus de Hawkes multivariés : chaque événement augmente la probabilité d'occurrence d'un nouvel événement, au sein du même groupe - même secteur ou type d'attaques (auto-excitation), et chaque événement au sein d'un groupe augmente potentiellement la probabilité d'occurrence d'un nouvel événement au sein d'un autre groupe (inter-excitation). Une procédure d'inférence pénalisée peut être alors développée pour capturer les interactions pertinentes entre les différentes classes d'événements et prédire la distribution jointe du nombre d'attaques en fonction de leurs caractéristiques, comme dans [BBH20].

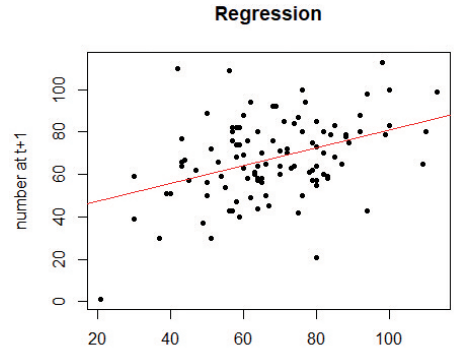
Il s'agit d'une première étape dans la quantification de la composante fréquence du risque cyber. Néanmoins, pour capturer pleinement la composante fréquence, il faudrait également disposer d'informations sur l'exposition, ce qui est très délicat à partir de base de données publiques comme la base PRC : en effet, quelle partie de la variation dans le temps des sinistres déclarés est causée par une évolution du risque, et quelle partie est causée par une instabilité dans la manière dont les données sont collectées ? Connaitre l'exposition nécessite de suivre au cours du temps le nombre d'entités exposées au risque cyber, tout en s'assurant de l'exhaustivité du processus de déclaration des sinistres au sein de la base de données publiques. À enrichir avec les données assureurs qui ont une meilleure expertise sur l'exposition, tout en ayant moins d'expérience sur la sinistralité que les bases publiques.

Encadré 5 : Base de données Privacy Rights Clearinghouse (PRC)

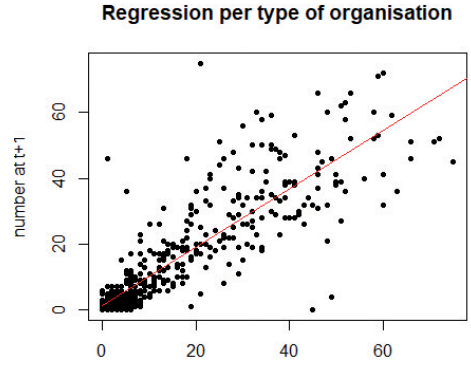
La base de données Privacy Rights Clearinghouse (PRC) est une base de données publique rassemblant des violations de données ciblant l'industrie américaine, ainsi que différentes caractéristiques comme le nom de l'entité ciblée et son secteur d'activité, sa localisation, la date de déclaration de la violation, le type de violation, le nombre de personnes affectées, la source d'information qui a remonté la violation de données à la base (agences gouvernementales américaines, organisations à but non lucratif, médias …). Une indication de gravité est également donnée via le volume de données violées, ce qui est utile pour les applications en assurance.

Cette base a ainsi été utilisée et étudiée dans plusieurs références académiques sur le cyber-risque, comme [MS10], [FHE16], [EL17], [FLT21]. Néanmoins, cette base de données n'est pas alimentée par un portefeuille d'assurances, mais par diverses sources d'information, chacune rapportant des types de sinistres hétérogènes. En particulier, l'exposition, c'est-à-dire le nombre d'entités exposées au risque dans le périmètre de l'organisation de la PRC, est floue. Ainsi cette base publique PRC est à considérer avec précaution et est utilisée ici avant tout pour illustrer notre méthodologie, qui peut être facilement étendue à d'autres types de données.

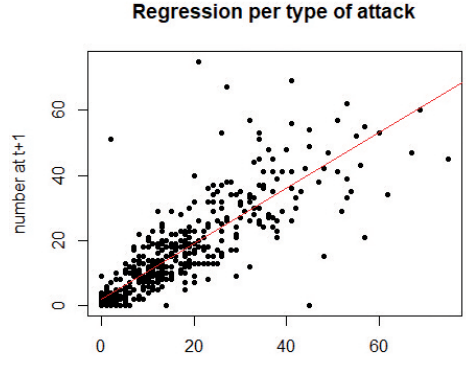
Figure 5 : Régression du nombre d'événements pendant le mois t+1 en fonction du nombre d'événements pendant le mois t
(Base PRC - Période 2010-2018)



R^2 = 0.164, Intervalle de confiance (95 %) [0.030, 0.278]



R^2=0.780, Intervalle de confiance (95 %) [0.750, 0.810]



R^2=0.726, Intervalle de confiance (95 %) [0.687, 0.766]

Encadré 6 : Processus ponctuels et intensité

Soit $N_t = \sum_{n\geq 1} 1_{T_n \leq t}$ un processus ponctuel où T_n est le temps du nième saut, caractérisé par son intensité de saut (aussi appelé taux de hasard) λ_t : l'intensité λ_t représente la "probabilité" d'avoir un saut à la date time t, étant donnée l'information passée.

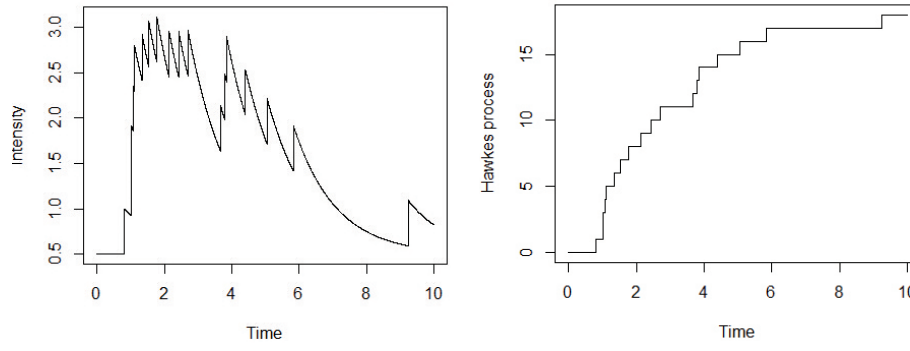
1. N_t est un processus de Poisson homogène, d'intensité de saut constante positive λ, si les durées inter-sauts $(T_n - T_{n-1})$ sont des variables aléatoires indépendantes et de même loi exponentielle de paramètre λ : $P(T_n - T_{n-1} > t) = exp(-\lambda t)$

2. N_t est un processus de Poisson non homogène, caractérisé par une intensité déterministe λ_t (positive) si les durées inter-sauts $(T_n - T_{n-1})$ sont indépendantes, de loi donnée par
$$P(T_n - T_{n-1} > t) = exp\left(-\int_0^t \lambda_s ds\right)$$

3. N_t un processus de Hawkes de fonction d'excitation ϕ (fonction déterministe positive) est caractérisé par une intensité stochastique λ_t définie par $\lambda_t = \mu_t + \sum_{T_n<t} \phi(t - T_n)$, avec μ_t fonction déterministe (positive).

Pour un processus de Hawkes, l'intensité λ_t est donc caractérisée par une intensité de référence μ_t qui représente le taux auquel arrive un saut de façon "spontané", plus une partie d'auto-excitation $\sum_{T_n<t} \phi(t - T_n)$, où ϕ est la fonction (ou noyau) d'excitation du processus de Hawkes, qui traduit le fait que les sauts passés influencent également l'occurrence d'un saut en la date t.

Figure 6 : Une trajectoire d'un processus de Hawkes univarié et son processus intensité correspondant.
Chaque saut représente un événement. Le noyau d'excitation utilisé ici est la fonction exponentielle $\phi(s) = \alpha exp(-\beta s)$: ainsi on observe bien que l'intensité décroit de façon exponentielle entre les sauts.



3.2. Risque d'accumulation de sinistres cyber

Le potentiel systémique du risque cyber repose également sur la possibilité d'une défaillance simultanée d'une proportion massive d'assurés. Un rapport de Cyence et Lloyd's of London [L17] a ainsi estimé que, si un sinistre survenait chez un prestataire de cloud, le coût de l'attaque se situerait dans une fourchette de 15 à 121 milliards d'USD, avec une perte moyenne estimée à 53 milliards. Un exemple de telle cyber attaque massive est l'attaque du rançongiciel Wannacry en mai 2017 qui a conduit à une contagion d'environ 300 000 ordinateurs dans plus de 150 pays (cf. Encadré 1). Il est important de noter que même si le coût de chaque sinistre en lui-même est faible, la survenance simultanée d'un grand nombre de sinistres lors d'une attaque massive peut induire des coûts cumulés très élevés. Ce type de crises, appelés "scénario d'accumulation", peuvent mettre en défaut le principe de mutualisation, qui est au cœur de l'activité d'assurance. En effet, dans ces situations, l'hypothèse d'indépendance des assurés, qui est l'hypothèse centrale de la Loi des grands nombres et qui sous-tend le principe de mutualisation, n'est plus vérifiée (cf. Encadré 2).

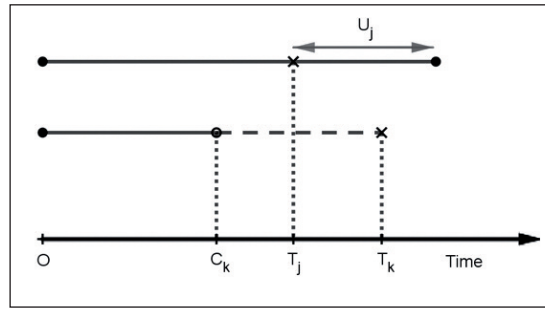
Par ailleurs, si un grand nombre d'assurés sont simultanément victimes d'une attaque, une saturation de la capacité de réponse de l'assureur peut se produire. En effet, les contrats cyber incluent généralement, en plus de la réparation financière, des prestations moins usuelles pour le secteur, puisqu'ils sont couplés avec des offres de prévention et d'assistance en cas de sinistre (par des équipes d'experts comme des cabinets de cyber-sécurité) pour aider l'assuré dans sa reprise d'activité. Cette assistance se doit d'être rapide et particulièrement réactive, afin d'éviter une aggravation des dommages. L'incapacité de l'assureur à intervenir de manière appropriée dans un délai court peut induire des pertes supplémentaires, comme des sanctions financières, une perte de réputation, mais aussi des dommages accrus pour les assurés, laissés seuls sans assistance. Pour répondre à ces engagements, l'assureur doit donc pouvoir anticiper le niveau de réponse nécessaire au cours d'une telle crise.

La conception de scénarios d'accumulation est donc un véritable enjeu pour l'assurabilité du cyber-risque, afin d'anticiper l'impact d'une cyber-attaque massive sur un portefeuille d'assurances et évaluer sa résilience. [HL21] propose une méthodologie générale et flexible qui peut aider les compagnies d'assurance à concevoir leurs stratégies face à de tels cyber-ouragans et à dimensionner la capacité de réponse (en termes de prévention et temps de réaction à l'attaque).

La construction de ces scénarios d'accumulation de [HL21] repose sur des modèles stochastiques épidémiologiques de contagion qui sont adaptés au contexte du cyber risque : c'est un modèle de contagion de virus, comme ceux utilisés pour la pandémie de Covid-19. Les gestes barrières, la vaccination, sont ici remplacés par d'autres mesures de prévention, comme l'identification et la correction des vulnérabilités. Le risque de saturation des services de réanimation est ici remplacé par le risque de ne pas pouvoir fournir toute l'assistance nécessaire aux assurés. À noter que malgré ces analogies entre épidémie cyber et épidémie biologique, des différences subsistent, en particulier concernant les échelles temporelles, les valeurs des paramètres, ainsi que la nature du risque. Cela nécessite donc une adaptation des modèles existants au contexte cyber.

Pour apporter de la flexibilité à la modélisation, celle-ci est séparée en trois parties disjointes (cf. Encadré 7) :

Encadré 7 : Modélisation micro de la cyber-épidémie : chronologie des événements pour un assuré j et un assuré k



Pour un(e) assuré(e) donné(e), on définit :

T = date à laquelle l'assuré(e) est infecté(e) (peut être $+\infty$),

U = durée de l'assistance après infection,

C = temps au bout duquel l'assuré(e) applique un correctif qui empêche l'infection.

1. **Le module "environnement"** qui correspond à modéliser la variable aléatoire T, ie la sévérité de l'infection dans la population globale.
2. **Le module "réparation"** : modéliser la variable aléatoire U, qui représente le temps d'intervention immédiate pour "apporter les premiers soins", et qui dépend du type d'infection modélisée (ransomware, corruption de données…).
3. **Le module "prévention et réponse"** : modéliser la variable aléatoire C qui représente la réactivité des acteurs à détecter la menace et à mettre en œuvre une riposte.

Pour le module environnement, un modèle à compartiments de type SIR (susceptible, infecté, guéri ou *recovered*), peut être utilisé (cf. Figure 7). Celui-ci est caractérisé par deux paramètres : le taux d'infection noté β, et le taux de guérison noté γ. Le nombre de reproduction $R_0 = \beta / \gamma$ caractérise la virulence de l'épidémie : si $R_0 < 1$ il y a extinction, en revanche si $R_0 > 1$ l'attaque se propage. Ce que l'on appelle ici guéris sont les assurés qui n'ont plus besoin d'une assistance à court terme, et donc ne contribuent plus à la saturation de la réponse de l'assureur ; une guérison "totale" pouvant quant à elle être bien plus longue.

Les effectifs S, I et R des trois compartiments satisfont le système d'équations différentielles.

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

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

$$\frac{dR(t)}{dt} = \gamma I(t).$$

Nous avons choisi de présenter ici le modèle épidémiologique de contagion SIR, qui a vocation à être simple, mais dans lequel notamment les effets de réseau sont absents, ou, du moins, pas évidents puisque dilués dans une vision collective macro de la cyber-épidémie. Bien entendu, les structures de réseau peuvent avoir un impact important sur les pertes liées au cyber-risque. Pour les matérialiser, on peut remplacer, par exemple, le modèle SIR par un modèle SIR multi-groupes dans lequel les assurés sont séparés en différentes catégories. Les liens entre les différentes catégories peuvent être plus ou moins forts, ce qui induit une matrice de coefficients dont les valeurs matérialisent le réseau : les catégories plus connectées sont associées à des paramètres de contagion plus élevés. Par ailleurs, il est également possible de modéliser des attaques non contagieuses, puisqu'un taux d'attaque homogène peut également être utilisé pour modéliser la variable aléatoire T, et qui correspond également à certains schémas d'événements, comme certaines campagnes massives de spams. Néanmoins, il faut souligner la difficulté de calibration des scénarios de cyber-attaques, en particulier car les informations sur les structures des réseaux sont presque impossibles à obtenir, notamment pour les petites entreprises.

Dès que la menace a été détectée (par exemple après un délai de quelques jours) et que les correctifs sont identifiés, les assurés peuvent les implémenter. Différentes dynamiques de réaction au cours du temps peuvent être considérées : par exemple un taux d'implémentation constant (correspondant à une loi de type exponentielle), décroissant (loi de type Pareto), ou bien croissant (loi de type Weibull), (cf. Figure 8).

Une fois ces trois modules implémentés, différents indicateurs de suivi du risque peuvent être analysés, en ayant au préalable ajustés les paramètres du modèle épidémiologique à la cinétique de Wannacry, cf. [HL21]. Par exemple, la Figure 9 représente, pour 10 000 scénarios, l'évolution au cours du temps du nombre de victimes lors d'une cyber-attaque de type Wannacry en fonction de la rapidité de la réponse et la forme des réactions d'implémentation des contre-mesures. Nous pouvons ainsi visualiser la réduction du pic en fonction du comportement. On constate que ce qui compte n'est pas tant la forme de la réaction, mais surtout la rapidité de la réponse qui est crucial pour réduire le risque de saturation : une réponse lente ne diminuera guère la charge des équipes d'assistance (réduction d'environ 4 % seulement), tandis qu'une réponse rapide en 3 jours réduit considérablement (jusqu'à 30 %) le pic du nombre d'assurés nécessitant une assistance. Néanmoins, une réaction, même plus lente, aura toujours un effet bénéfique sur le nombre total de victimes.

En conclusion, le cadre de construction de scénarios d'accumulation présenté ici est flexible et peut facilement se généraliser à tout autre type de modèles pour la dynamique de l'attaque, la qualité de l'intervention du prestataire (la durée de guérison), ou pour représenter les comportements des assurés vis-à-vis de la prévention. Par exemple, la dynamique de l'épidémie, c'est-à-dire le modèle de contagion, peut quant à lui être facilement enrichi si l'on souhaite introduire des effets réseaux, matérialisant une plus grande contagion entre certains secteurs d'activité plus connectés que d'autres. Par ailleurs, une attention particulière doit être portée à la définition de scénarios globaux réalistes pour décrire une telle cyber-épidémie. Pour l'instant, il y a un manque de données publiques pour identifier clairement les chronologies précises des cyber-attaques massives. L'exemple pris ici, inspiré de la crise de Wannacry, ne doit être considéré que comme une référence grossière, en raison du nombre d'hypothèses qui ont été faites pour tenter de reproduire cet épisode.

Figure 7 : Modèle épidémiologique SIR

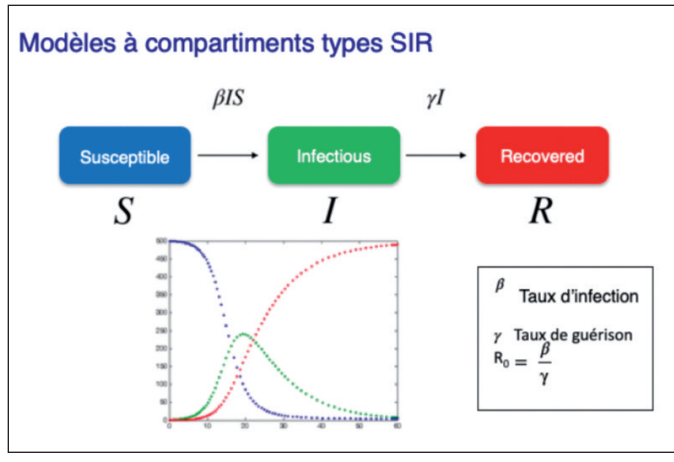


Figure 8 : Différentes dynamiques des taux d'implémentation des mesures de protection

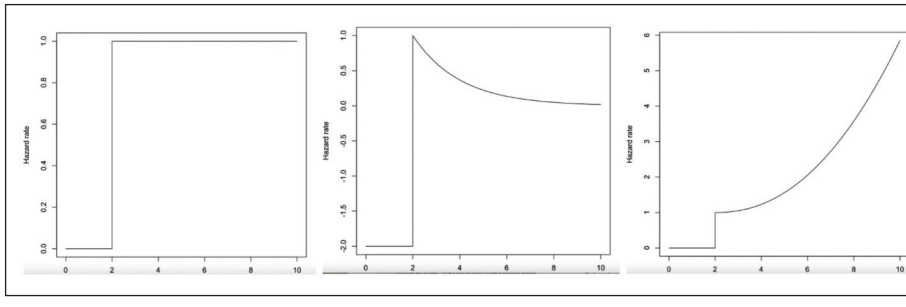
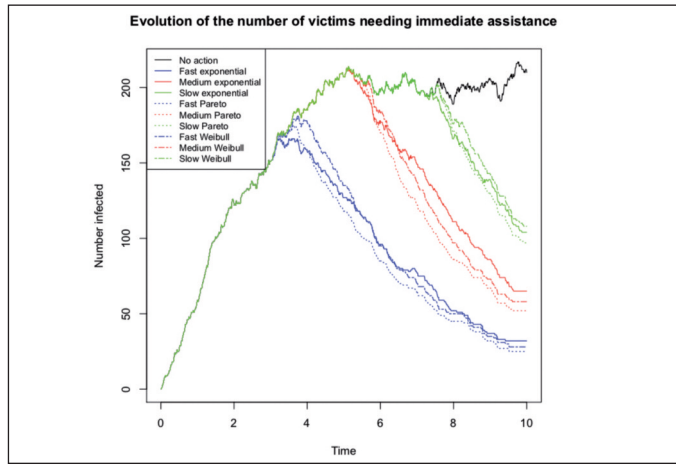


Figure 9 : Evolution au cours du temps du nombre de victimes ayant besoin d'assistance



IV Bases de données, et aspects comportementaux des victimes et acteurs malveillants

4.1. Pour un observatoire du cyber-risque

Il existe peu de sources de données publiques permettant un suivi en temps réel du cyber-risque. Le GIP Acyma, à travers sa plateforme cybermalveillance.gouv.fr, collecte et produit des statistiques qui permettent, via ses publications et ses rapports d'activité, d'obtenir des informations quantitatives sur l'évolution de la menace. C'est aussi le cas des publications de l'ANSSI, parmi lesquelles on peut citer notamment le rapport sur les rançongiciels [ANSSI21b]. L'AMRAE, via son étude "Lumière sur la cyber-assurance" (dite "Lucy") [LUCY21], a produit un travail considérable de recensement des sinistres indemnisés par les assureurs via une enquête auprès des courtiers. Les productions de ces différentes sources de données sont extrêmement précieuses en vue de la quantification du risque, sur des périmètres différents et complémentaires.

Néanmoins, ces statistiques n'ont pas encore la maturité nécessaire pour apporter une vision suffisante du risque, et réagir rapidement à ses évolutions.

Par manque de maturité, nous entendons soit l'absence d'informations très précises sur le risque, soit les imprécisions sur les méthodes de collecte et leur stabilité dans le temps, qui permettraient de s'assurer de la fiabilité des données et de leur suivi dans le temps. Pour prendre l'exemple du rapport de l'ANSSI sur les rançongiciels, plusieurs informations précieuses sur les proportions d'attaques proviennent de sources peu ou mal précisées, certaines reprises de rapports de sociétés de cyber-sécurité dont la méthodologie de production des statistiques est opaque. Un autre exemple éloquent concerne l'étude des profits générés par les rançongiciels (voir [ANSSI21b]). Les montants évalués sont entachés d'une marge d'erreur parfois importante, comme c'est le cas du logiciel Cryptowall dont les pertes générées sont estimées entre 18 et 320 millions de dollars. C'est moins l'amplitude de cette marge d'erreur qui interroge - elle est tout à fait compréhensible étant donné la complexe évaluation des profits d'organisations criminelles y compris clandestines – que la source de cette information, qui est mal connue. Ce manque d'information s'explique bien entendu par le caractère extrêmement sensible du sujet, mais complique l'évaluation du risque.

Par ailleurs, le cyber-risque évolue de façon extrêmement rapide. L'augmentation, début 2021, en quelques mois, du nombre de cyber-attaques en est un bon exemple. Or la fréquence de mise à jour de ces statistiques n'a pas aujourd'hui la même rapidité.

Afin de mieux identifier ce qui manque, à l'heure actuelle, dans le secteur du cyber, il nous paraît intéressant de comparer avec un autre type de menaces, qui concerne le champ de la veille sanitaire. Le choix de ce parallèle n'est pas anodin. Le terme même de "virus informatique" pose d'emblée une analogie entre les épidémies biologiques et le fonctionnement des infections cyber. Par ailleurs, l'épidémiologie est un champ où la fiabilité des données ne va pas de soi. Dans le cas du suivi d'un virus biologique, on ne dispose pas nécessairement des outils et méthodes de recensement des cas. De plus, des erreurs de diagnostics peuvent introduire des erreurs.

Le réseau Sentinelles (voir https://websenti.u707.jussieu.fr/sentiweb/) est un exemple de construction d'un outil statistique de recensement et de suivi de données liées à une menace changeante, et fortement dépendante du comportement humain. Via, notamment, des rapports publics hebdomadaires, le réseau assure le suivi sur les infections respiratoires aiguës (grippe avant l'irruption du Covid-19), les diarrhées aiguës, et la varicelle. D'autres indicateurs pathologiques sont également recensés, s'intégrant aux dispositifs de surveillance de Santé Publique France.

Derrière des initiatives comme Sentinelles, débutée en 1984, c'est toute une culture et un savoir-faire de la donnée de santé publique qui se révèlent extrêmement précieux en cas de crise. Par exemple, entre 1987 et 2002, l'outil s'adapte en intégrant des informations précieuses sur les tests VIH qui n'étaient pas dans le périmètre initial des infections ciblées. Lors de l'épidémie de Covid-19, les données publiques transmises quotidiennement par Santé Publique France (disponibles sur https://dashboard.covid19.data.gouv.fr/vue-d-ensemble?location=FRA) sont notamment nourries par cette expérience de la donnée, et se caractérisent par une rigueur exemplaire eu égard à la complexité du problème : on notera ainsi la documentation systématique accompagnant chaque publication de données, et rectifiant au besoin de façon transparente les erreurs constatées dans certaines extractions.

Ce degré d'informations manque aujourd'hui au suivi de la menace cyber et à l'anticipation de ses évolutions. Rappelons que, dans le domaine de la cyber-assurance, cette anticipation est cruciale, puisque la tarification, ainsi que le provisionnement reposent sur une prédiction des charges futures. Par ailleurs, la prévention, qui est un élément important de la réduction de la menace, bénéficierait fortement d'un baromètre en temps réel, d'autant que l'échelle temporelle du cyber-risque est assez courte.

Des sociétés de sécurité informatique proposent (voir notamment Kaspersky, https://cybermap.kaspersky.com/) différentes mesures en temps réel, mais leur exploitation est difficile du fait de la difficulté à quantifier leurs biais, et à l'absence de documentation précise sur leur méthodologie.

4.2. Aspects comportementaux

Dans son rapport d'activité 2020, Cybermalveillance [ANSSI21a] a qualifié la crise du Covid-19 "d'effet d'aubaine" pour les cyber-criminels. Dès les premières mesures de confinement mises en œuvre en Europe, on a noté ainsi une augmentation significative des menaces cyber en lien avec la maladie (voir [LSN21+]) : dès avril 2020, un nombre conséquent de sites malicieux ou de mails frauduleux ont tenté d'exploiter le filon de l'épidémie. À cela s'ajoute un passage massif et pas toujours anticipé au télétravail, qui a conduit à une utilisation non sécurisée d'outils numériques personnels dans un contexte professionnel, accroissant la vulnérabilité, voir [BS20]. Enfin, les attaques liées à la santé se sont multipliées, on peut notamment citer celle contre l'Agence Européenne du Médicament (voir https://www.ema.europa.eu/en/news/cyberattack-ema-update-5) dans le contexte de la validation des vaccins. Si les institutions de santé sont historiquement très exposées (le NHS a ainsi été l'une des victimes les plus médiatisées de la cyber-attaque Wannacry en 2017 [GKH+19]), le contexte sanitaire, en les plaçant au premier plan, peut expliquer pour partie la multiplication des attaques les concernant.

Derrière cet exemple de la crise du Covid-19, on trouve l'une des caractéristiques les plus inquiétantes du cyber-risque : la grande force d'adaptation des hackers, leur remarquable opportunisme. Ainsi, si le terme de "cyber-ouragan" (utilisé par exemple par l'Institut Montaigne dans son rapport [M18]) est souvent employé pour qualifier la dimension catastrophique du risque, cette catastrophe n'est précisément pas une catastrophe naturelle.

Il s'agit, en effet, d'un risque de nature humaine, nécessitant une meilleure compréhension des comportements des acteurs. En assurance, l'importance du comportement de l'assuré est bien connue. Les phénomènes d'antisélection et d'aléa moral (voir [P78]) sont une problématique importante de l'économétrie de l'assurance. L'antisélection a trait à un comportement précédant la souscription : pour qu'un assuré entame le mouvement vers l'assurance, il doit être plus sensible au risque, donc se trouve plus exposé qu'un individu moyen dans la population générale. L'aléa moral reflète un changement de comportement après la souscription, l'assuré se considérant protégé par son contrat opte pour une attitude moins prudente. À l'inverse, l'assureur, en effectuant de la prévention, parie sur le comportement vertueux de son client pour limiter ses pertes.

Dans le domaine des risques naturels, la prévention donne des résultats intéressants sur la réduction du risque, cf. [P18]. Transposer ce modèle dans le contexte cyber paraît indispensable. Néanmoins, l'extrême plasticité des criminels fait craindre une plus grande instabilité de la menace. Dans le cas des risques naturels, des évolutions ont bien entendu été constatées notamment en lien avec celles des phénomènes climatiques, mais ces changements, aussi préoccupants soient-ils, se projettent sur un horizon temporel plus long que dans le cas du cyber. Ainsi les augmentations de 255 % des attaques par ransomware en 2020, d'après [ANSSI21a], sont brutales. Afin de le comprendre et de l'anticiper, il devient donc nécessaire de mieux connaître les attaquants et leurs modes opératoires.

4.3. Modes opératoires

Le rapport d'activité 2020 de Cybermalveillance [ANSSI21a] fournit quelques indicateurs sur les principaux types d'attaques qui ont été remontés à la plateforme. L'hameçonnage (représentant 17 % des signalements à Cybermalveillance) apparaît comme le vecteur principal, reflétant une nouvelle fois l'importance du comportement des victimes : c'est l'erreur de la victime, cliquant sur un lien frauduleux, qui assure le succès de l'attaque. Mais cette menace est difficilement discernable (ainsi que le mentionnent les auteurs du rapport) de la seconde catégorie, recensée derrière le terme de "piratage de compte," celui-ci pouvant être causé à la suite de l'hameçonnage (typiquement, la victime transmet ses identifiants après la réponse à un mail frauduleux). Cette difficulté de nomenclature précise des incidents est un frein à l'exploitation efficace des statistiques sur le sujet.

Il est intéressant de noter, dans les chiffres de Cybermalveillance, que les "chantages à la webcam" représentent une part non négligeable des signalements (8 % environ). Ce phénomène, particulièrement médiatisé à travers l'affaire dite du "Cryptoporno" (voir https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/chantage-a-lordinateur-ou-a-la-webcam-pretendus-pirates) nécessite un très faible niveau technologique de la part de l'attaquant. Il s'agit d'une escroquerie classique où le criminel prêtant avoir piraté la webcam de la victime et le fait chanter, menaçant de publier des vidéos compromettantes s'il n'obtempère pas. Le succès repose alors essentiellement sur la crédulité de la cible, la webcam n'ayant pas nécessairement été piratée.

Ce type d'incidents frappe essentiellement les particuliers, qui, à l'heure actuelle, ne sont pas le cœur de cible des produits de cyber-assurance, tournés vers l'entreprise. Néanmoins, il est important de s'y intéresser, car elles révèlent l'efficacité de méthodes d'attaques peu techniques. Les entreprises peuvent ainsi elles aussi être frappées par des escroqueries qu'on pourrait qualifier de traditionnelles, en ceci qu'elles existaient avant l'ère informatique, mais transposées dans un cadre numérique. La "fraude au président" en est un bon exemple, et concerne typiquement une usurpation d'identité où un malfaiteur se fait passer pour un haut responsable d'une entreprise et obtient ainsi un virement frauduleux. Il s'agit plus ici de manipulation que de piratage, même si le vecteur numérique est utilisé.

On retrouve cette importance de l'ingénierie sociale dans les "Big Game Hunting". Ce type d'attaques de grande ampleur, décrites notamment dans le rapport de l'ANSSI sur les rançongiciels [ANSSI21b], nécessitent une préparation considérable des hackers. Plusieurs vecteurs sont utilisés afin d'infiltrer l'entreprise (numériquement mais parfois physiquement) et de générer ainsi un maximum de dommages, poussant la victime à payer la rançon. L'attaque par rançongiciel peut, par ailleurs, être renforcée par des attaques par déni de service pouvant paralyser une partie du réseau.

Si ce type de braquage numérique à grande échelle requiert un fort degré de professionnalisme de la part des criminels, toutes les attaques ne sont pas de cet acabit. L'émergence du "Ransomware as a service" (voir [MBS20]) vise à fournir des kits de piratage permettant à des individus malintentionnés de générer des dommages sans pour autant nécessiter un haut niveau en informatique.

4.4. Acteurs de la cyber-criminalité

Le phénomène "Ransomware as a service" révèle également l'importance du modèle économique sur lequel prospère l'écosystème cyber-criminel. En 2017, Wannacry [MP17] génère plusieurs centaines de millions de dollars de pertes, mais le montant de rançons ne s'élève qu'à 100 000 euros à peine (voir https://github.com/rwillmann/WannaCry-Outbreak-Data-12-May-2017—-19-May-2017), ce montant étant connu car les transactions sur les adresses bitcoin concernées sont publiques. À travers le RaaS, les criminels imaginent un système d'abonnement, les usagers payant des royalties aux auteurs. Ceci permet notamment à certains rançongiciels de générer des profits bien plus importants sur une période étendue : 6 millions de dollars estimés pour SamSam ente 2016 et 2018, entre 7,8 et 150 millions pour Locky entre 2016 et 2018, ou encore 150 millions pour GandCrab entre 2018 et 2019.

Par ailleurs, certains acteurs se positionnent entre le criminel et sa victime, flirtant avec la légalité. Le rapport de l'ANSSI [ANSSI21a] pointe ainsi la société qui se propose d'aider la victime à payer sa rançon, et a conclu des partenariats avec certains groupes de hackers pour obtenir des rabais sur le paiement de la rançon.

Une meilleure compréhension du modèle économique de ces acteurs est essentielle pour mieux anticiper l'évolution du risque et contrecarrer ses dérives. Dans le cas des rançongiciels, objectiver l'impact néfaste du paiement des rançons sur la prolifération des attaques serait un élément important pour définir une stratégie permettant de casser l'évolution de cette menace.

D'autant que l'écosystème de la cyber-criminalité est complexe, et les motivations des hackers ne sont pas seulement économiques. Le rançongiciel NotPetya [F18], ciblant à

l'origine l'Ukraine (la Russie étant soupçonnée d'en être l'auteur, voir https://www.lemonde.fr/pixels/article/2018/02/15/virus-informatique-notpetya-le-royaume-uni-accuse-la-russie-qui-dement_5257443_4408996.html), montre, si l'en est besoin, l'importance de la géopolitique dans les cyber-attaques. On retrouve des soupçons d'intervention étrangère dans l'attaque massive frappant l'Australie en 2020 (https://www.lemonde.fr/international/article/2020/06/19/l-australie-se-dit-victime-d-une-cyberattaque-d-un-acteur-etatique_6043366_3210.html), ou encore des soupçons d'espionnage derrière l'affaire Solar Winds [NYSDFS20].

À cela s'ajoute les motivations de nature idéologique et non financière, on parle parfois de cyber-hacktivisme. On peut y rattacher, par exemple, le piratage du site de rencontres Ashley Madison en 2016 (voir [MD15]) ou des motivations religieuses comme dans le cas de l'opération Ababil (voir [I13]).

Ces exemples dessinent un paysage complexe, avec une certaine porosité entre ces différentes classes de cyber-criminels, comme pointé par l'ANSSI [ANSSI21a]. De même que, dans le domaine climatique, il est important d'étudier les causes naturelles pour prévoir leur évolution, la compréhension de cet éco-système et de son évolution est fondamentale si l'on veut passer de la réaction à l'anticipation.

V Conclusion

Face à la montée inexorable du risque-cyber, l'assurance apparaît comme un outil incontournable pour augmenter la capacité de résilience du tissu économique et industriel face à ces attaques. Mais si le marché de la cyber-assurance se développe - en mettant en avant des offres innovantes qui couplent prévention, réparation financière, et accompagnement en cas de crise - il devient particulièrement tendu, que ce soit en termes de renouvellement des contrats, ou de souscriptions des PME/ETI dont le taux de couverture a du mal à décoller. Cette sous-couverture fait courir des risques aux entreprises et aux collectivités publiques concernées, mais aussi à l'ensemble de leur écosystème : sous-traitants, fournisseurs, clients, partenaires commerciaux...

En outre, de nombreuses questions se posent sur la viabilité du marché de la cyber-assurance et sur la capacité du secteur à mutualiser les pertes en cas de sinistre majeur. Différents facteurs mettent en péril cette mutualisation :

- La difficile quantification, et donc anticipation, des impacts face à un risque émergent en rapide évolution.
- Le périmètre mouvant du risque, notamment à travers le "cyber silencieux".
- L'extrême volatilité des dommages d'un incident cyber à l'autre.
- Le caractère systémique du risque, une "cyber-pandémie" pouvant entraîner la défaillance simultanée de nombreux assurés.

Avec un tel niveau d'incertitude, la construction de modèles statistiquement fiables requiert un nombre important de données. Sans base de données fiables et riches, il est difficile d'envisager qu'un équilibre économique se fasse, où chaque compagnie parviendrait à une évaluation du risque basée uniquement sur son expérience individuelle. L'exploitation et l'aggravation de ce déséquilibre est au contraire au cœur de la stratégie des acteurs malveillants à l'œuvre derrière les incidents cyber. En outre, l'évolution des comportements au sein de l'éco-système cyber (hackers, usagers, acteurs de la protection) empêche une rapide stabilisation. Face à cette incertitude, la solution purement juridique visant à exclure des contrats certains types d'événements, et à introduire des limites d'indemnisation rendant moins attractives les garanties, n'est pas satisfaisante : d'une part l'objectif de résilience de l'économie devient plus difficile à atteindre, d'autre part cet appauvrissement des garanties freine le développement du marché de l'assurance cyber, et, paradoxalement, accroît les risques des assureurs en bridant leur capacité de mutualisation.

Dans ce contexte, le partage d'information nous paraît essentiel. Le risque cyber est un risque foncièrement humain, construit sur une compétition entre des agresseurs (les cyber-criminels) et une société qui cherche à se protéger tout en bénéficiant des apports de la révolution numérique. Dans le cadre de cette opposition, les attaquants pratiquent à leur manière le partage d'informations et de savoir-faire, mettant en commun des techniques, jusqu'à des packages clé en main dans le cadre du "Ransomware as a service". Le camp des défenseurs doit rattraper son retard dans ce domaine d'échanges d'information. La constitution de bases de données mutualisées entre acteurs de la défense cyber (assureurs, pouvoirs publics, acteurs de la cyber-sécurité…) nous paraît essentielle en vue de la constitution d'un modèle économique viable pour l'assurance. Le cloisonnement des informations - par exemple dans l'espoir vain d'en tirer un avantage concurrentiel - nous paraît à contretemps de l'urgence d'une meilleure quantification et anticipation collective de ce risque.

Cyber insurance: issues, modelling and mutualisation levers

Caroline Hillairet
ENSAE Paris, Centre de Recherche en Économie et Statistique

Olivier Lopez
Sorbonne Université, ISUP, Laboratoire de Probabilités, Statistique et Modélisation

Abstract

The growth of the digital economy has brought about profound transformations in most economic sectors. These changes have modified the mapping of risks faced by companies, especially those related to information systems. In the past few years, cyber risk has emerged as one of the main threats to businesses, as indicated in particular in the report by the Ministry of the Interior [RM19] on the subject. Insurance is therefore a tool that can strengthen the resilience of the economy in the face of this major risk, and even contribute to cyber defence. But although the cyber insurance market is developing – by offering innovative policies that combine prevention, financial compensation and support in the event of a crisis – many questions are being asked regarding the viability of these offerings, and about the sector's capacity to mutualise losses in the event of a major disaster. In this article, we discuss the technical issues involved in quantifying cyber risk. We explain how appropriate mathematical modelling can contribute to a better assessment of risk and the viability of the cyber insurance economic model. The relevance of such modelling is currently constrained by the limited data available. We make recommendations for the sharing of information between actors, an essential condition for society's resilience to cyber threat.

The study reflects the personal views of its authors and does not necessarily express the position of the Institut Louis Bachelier and the Louis Bachelier Finance and Sustainable Growth Laboratory of Excellence.

I. Introduction

With the growth of the digital economy, cyber risk has become one of the main threats to businesses (see in particular the 2019 report of the Ministry of the Interior [RM19]). According to Jerome Powell, President of the U.S. Federal Reserve, cyber-attacks now constitute the main threat to the global financial system. This threat has been amplified since the health crisis linked to the Covid-19 pandemic, as pointed out in the 2020 activity report of the French National Agency for Information Systems Security (ANSSI) [ANSSI21a], which concludes that there has been a massive increase in cyber-attacks, particularly ransomware, with a fourfold increase in the number of reports between 2019 and 2020.

In the face of cyber-risk, insurance has a crucial role to play in terms of compensation, particularly financial compensation. Physical cyber security, which is essential for limiting and preventing attacks, cannot be an impenetrable barrier against them. But for economically viable financial protection to emerge, it is necessary to quantify the impact of this risk. Multi-faceted risk assessment requires advanced statistical and probabilistic techniques for foreseeing the costs, the evolution of the threat and its financial impacts, in order to overcome the challenges inherent in cyber insurance.

In order to better understand these issues, we first describe the nature of risk through examples of significant cyber events, before presenting some descriptive features of the current cyber insurance market.

1.1. Description and examples of cyber-attacks

Cyber-attacks are a phenomenon as old as computing itself. However, the increased reliance of economies on digital technology, as well as the increased connectivity of economic agents, has changed the nature and impact of these events. Wannacry (see [MP17] and Box 1) and NotPetya (see [T17] and [F18]), which took place just a few weeks apart, are two outstanding examples of massive attacks. In the space of a few days, Wannacry hit around 300,000 computers in 150 countries, and NotPetya several million in 65 countries. The resulting losses were substantial, though it is difficult to quantify them precisely. Estimates range from several hundred million to 4 billion dollars for Wannacry, see [EUROPOL18], and more than 10 billion dollars for NotPetya, see [B20] and [CISA20]. The difficulty in quantifying the costs is due in particular to the fact that the indirect consequences suffered by the victims may sometimes be greater than the immediate damage. According to Bruno Charrat, co-manager of the CEA's Cybersecurity programme, "1% of the world's GDP, i.e. 1,000 billion dollars, is lost every year to cybercrime". (see [CEA21])

These two high-profile attacks, Wannacry and NotPetya, are examples of ransomware. Ransomware infects an information system by exploiting a flaw, or vulnerability, in the system. Sometimes, in what is known as a "Zero Day Exploit", the vulnerability is discovered by the hackers, with the cyber security personnel being unaware of it. But most often, previously identified vulnerabilities are exploited, for which patches exist. This was the case of the Eternal Blue vulnerability (see [T17]), exploited by Wannacry and NotPetya, which could have been fixed by simply updating the systems before the crisis. Once introduced via the flaw, the virus blocks access to the information contained in the system and access is only restored once the ransom has been paid.[1]

[1] Restoration does not always occur. For example, in the case of Wannacry, payment failed to unlock the information system, see [MP17]. More recently, Colonial Pipeline, despite paying a ransom of 4 million dollars, did not recover all its data, see [E21].

As already mentioned, the damage associated with these attacks is usually not only related to the ransom itself. In the case of Wannacry, the amount of the ransoms is known, as the transactions on the bitcoin addresses are public and their destination cannot be traced. Nevertheless, the cost of the ransoms themselves is very low compared to the total loss, which results from the interruption to operations, as in the case of the Colonial Pipeline attack (see [E21]), or from the legal and reputation risks. This is particularly the case when a 'double extortion' attack occurs, in which the blocking of data is preceded by its exfiltration, with the threat of disclosure. If personal data is affected, this may fall under General Data Protection Regulation. Alternatively, confidential information or trade secrets may be revealed.

1.2. The cyber insurance market

Cyber insurance policies were first offered in the 1990s, in the form of packages (software + insurance), by security software publishers in partnership with insurance companies (see [BM09]). Over the years, the stand-alone cyber insurance market (where policies solely concern cyber risk) has developed, mainly in the U.S., with specific clauses, in order to adapt to the continuous evolution of cyber-attacks and the complexity of information systems. Data protection regulations (the first being the Data Breach Notification Act, passed in California in 2003) have also been an important driver of the cyber insurance market. A number of qualitative studies on cyber insurance policies, mainly from the U.S., have been published, such as [MMN+15] which compares the coverage provided by various insurance policies. More recently, [RAK+19] gives an overview of the U.S. cyber insurance market (specifically the states of New York, Pennsylvania and California) with respect to the losses covered by insurance policies, the questionnaires filled out at the time of purchase, and the factors used to calculate insurance premiums. Although the cyber insurance market in the U.S. is instructive because it is more mature, it does not fully transpose to the specific framework of the French market and more generally to the European market, particularly with regard to the extent of cases of personal data leakage.

Faced with this multifaceted risk, cyber insurance in Europe also includes various guarantees, typically:

- Coverage for repair of damage and restoring the information system.
- Business interruption cover.
- Civil liability coverage, in the event of personal data leakage, to comply with the European RGPD regulation (potential legal costs and fines).
- Coverage of communication costs in the event of a crisis, as a cyber incident can tarnish the company's image.

Nevertheless, despite these multiple guarantees, the true damage is not always included or anticipated in cyber insurance coverage, and can be very costly: for example, the death of a patient in 2020 following the cyber-attack on the University Hospital of Düsseldorf in Germany, even though investigations reclassified the event as "loss of life" and not homicide. Furthermore, a cyber-attack can trigger non-cyber insurance policy cover, such as fire, or an explosion, as was the case in 1982 following the hacking of the control systems of a Siberian gas pipeline.

In addition to financial compensation, cyber contracts generally include offers of prevention and assistance in the event of a loss. This prevention/assistance component is particularly useful for SMEs, which do not always have sufficient expertise to deal with cyber risks. Because insurers are only indirect observers of these events, their role at the time of an attack is often limited, compared to cyber security companies or the state. Nevertheless, they can be a valuable source of information for helping to reduce more constant threats. Furthermore, thanks to the questionnaires completed when policies are taken out and to the determination of the rate, insurance plays a key role in improving the insured party's knowledge of cyber risk and encouraging it to improve its cyber hygiene. These questionnaires and audits could also contribute to mapping risk, much like a virtual "zoner", for better diversification of risk and therefore better insurability.

In France, AMRAE's "Light upon cyber insurance" (LUCY) study also provides a clear overview of premiums collected in France as well as claims experience for 2019 and 2020. Based on broker data, the study [LUCY21], is one of the few reliable sources on the sector, although it does not capture claims that may have been incurred by VSEs/SMEs or ETIs.

While the market is developing and responding to a growing need, it is hampered by a number of difficulties, which may explain the slowdown in the take-up of insurance in France following significant growth: according to the annual OpinionWay surveys for the Club des Experts de la Sécurité de l'Information et du Numérique [CESIN], 19% of respondents took out cyber insurance in 2015, compared with 50% in 2019 and 60% in 2020. While 87% of large companies are now covered by a cyber insurance policy, the rate of coverage for VSEs, SMEs and public authorities is still very low (only 8% for SMEs, according to [LUCY21]). Yet these enterprises are particularly vulnerable to cyber risk, both in terms of their ability to analyse their own risk and to identify and implement good IT security practices and in terms of the financial cushion for absorbing the impacts of a cyber-attack.

One of the difficulties encountered by insurers is the need to redefine the scope of contracts, and in particular to identify, in non-cyber policies (e.g. civil liability policies), cases where a cyber incident could activate the cover. This situation – known as "silent cyber" cover – can in fact unbalance existing portfolios, the composition of which is not designed to withstand the serious consequences of a loss of this nature. The work of identifying silent cover is therefore accompanied by the construction of so-called "affirmative" cover, which can be included in dedicated cyber insurance policies.

But the challenges of the emerging cyber market are not limited to this issue of formulation or exclusion of certain events. AMRAE's LUCY study highlights the very much worse Loss Ratio (LR) for 2019 and especially 2020 (84% and 167% respectively). This LR ratio compares the amount paid out for claims to the premiums received to absorb them. In a balanced system, the premiums allow for the outgoings to be absorbed, and a low LR reflects good anticipation of the evolution of risk. AMRAE's extremely high figures underline the uncertainties faced by the sector and the difficulty of quantifying the risks involved.

In this article, we discuss why cyber risk and its financial impact is a difficult topic to grasp. We also provide a number of promising approaches for addressing these issues. In the first section, we place cyber risk in the extreme risk category, the study of which falls within the statistical theory of extreme values. Extreme risks are characterised by the very high volatility of the cost of each event.

But the extreme severity of a single victim event should not obscure the danger posed by the systemic nature of cyber risk, which we discuss in the second section. Because of its capacity to spread at the speed of fibre optics in communication networks, a cyber-attack can lead to contagion and massive failures that can bring an economy to a halt, or at the very least jeopardise the solvency of an insurer. We then go on to explain which recent models can be used to foresee countermeasures and their effects in response to this threat.

These models, which are essential for quantifying risk, raise questions about the data needed to calibrate them, as well as the methods to be used to monitor these evolving risks. We consider this question in the final section which looks at recommendations on the constitution of coherent information bases on risk and on the need to understand its behavioural aspects, linked in particular to the malicious ecosystem underlying the attacks.

Box 1: An example of a massive cyber-attack: the Wannacry ransomware

Access to the information contained in the server infected by the ransomware is blocked, and this screen appears, demanding a ransom to recover the data. The virus, which exploits the EternalBlue flaw, spread rapidly through the Internet and affected between 200,000 and 300,000 victims in 150 countries within a week. Victims included individuals, businesses of all sizes, and health services such as the UK National Health Service (NHS). The total impact amounted to around a billion dollars, and 92 million pounds sterling for the NHS alone. Even though the ransom itself was relatively low (between $300 and $600), the multiple losses incurred, as well as interruption to business, accounted for these enormous figures.

II. Extreme risks

The mutualisation mechanism is based on the law of large numbers (see Box 2), which assumes there is an expectation for the random variable representing the loss by an insured party. Its existence does not always hold, as the quantity can be infinite for certain variables known as "heavy tails", i.e. they can have large values with a non-negligible probability. This is the case, for example, for Pareto laws with a Pareto index γ (also called tail index) smaller than 1 (see Box 3 and Figure 3).

This may seem paradoxical for real phenomena: a loss is always bounded, even if extremely high. In particular, in the field of cyber insurance, compensation limits are regularly introduced. It should be remembered, however, that the issue is not only to have a finite expectation, To be able to insure a risk, the premium must be low enough to be sufficiently attractive. If the rate is too high, the insurance model ceases to be economically viable.

It should also be noted that in some situations, even if the loss is theoretically bounded, there may be very little statistical difference between the actual loss distribution and the heavy-tailed distributions used in extreme value theory (see for example [ABT17]). This kind of phenomenon can be seen in the cyber loss data collected by AMRAE in the framework of its study "Lumière sur la cyber-assurance" ("Light upon cyber insurance") (see reference [LUCY21]). Figures 1 and 2 show a very high disparity between claims, with a small number of claims being of substantial size compared to typical cases. This type of finding, indicating extreme cost volatility, suggests turning to so-called heavy-tailed distributions in order to model this variable.

The choice of a generalized Pareto distribution is not arbitrary, but guided by Extreme Value Theory (see [BGS+06]). This statistical field concerns the study and classification of the tails of distributions of random phenomena, i.e. zones of large values corresponding to pessimistic but not completely improbable scenarios. The tail index is the measure of the severity of such a phenomenon. A variable with low values will have a zero or even negative tail index: Gaussian distributions, which are widely used in probability because of their favoured role through the Central Limit Theorem (see Box 2), thus have a tail index of zero. On the other hand, particularly volatile phenomena are characterised by a strictly positive tail index. In such cases, the upper part of the distribution can, under reasonable conditions, be approximated by a Generalized Pareto distribution.

In the AMRAE data, the goodness-of-fit of a generalized Pareto law tends to support the hypothesis of a strictly positive tail index in the case of cyber claims costs. This type of phenomena has also been identified for cyber claims related to data leaks, see in particular [MS10] and [FTL21]. In particular, the pivotal value is 1: if the tail index exceeds 1, the expectation is infinite and the risk is "uninsurable" unless indemnity limits are introduced. The closer one gets to 1, the more critical the situation becomes, requiring a larger volume of insured parties to adequately cushion the risk.

Faced with such a situation, the most radical solution is to exclude the risk: if the risk is uninsurable, it might as well not be insured. Without fully adopting this position, it is possible to redefine the scope of policies, typically by introducing more restrictive indemnity limits.

This solution is nonetheless unsatisfactory. Firstly, it penalises the client by reducing the extent of coverage. And secondly it does not guarantee any better result for the insurer, who is still faced with a high volatility of results, unless ridiculously low limits are imposed that are at odds with the client's expectations. To absorb this volatility, a large number of policyholders will have to be reached, an objective that is all the more difficult as the benefits are not very attractive. A vicious circle is thus created.

Figure 1: Amounts of cyber claims
(source: LUCY study by AMRAE in 2021)

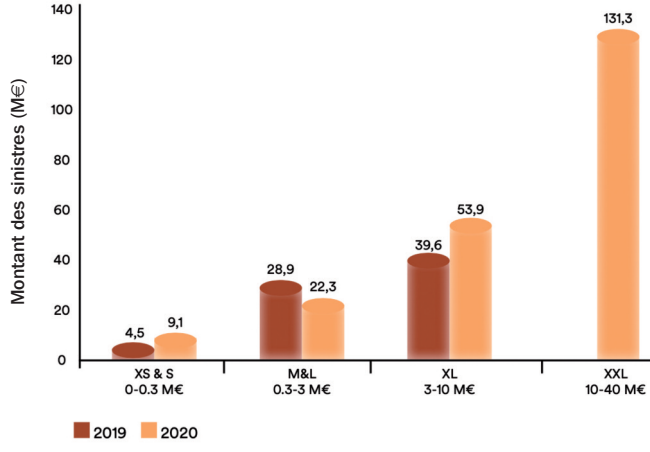
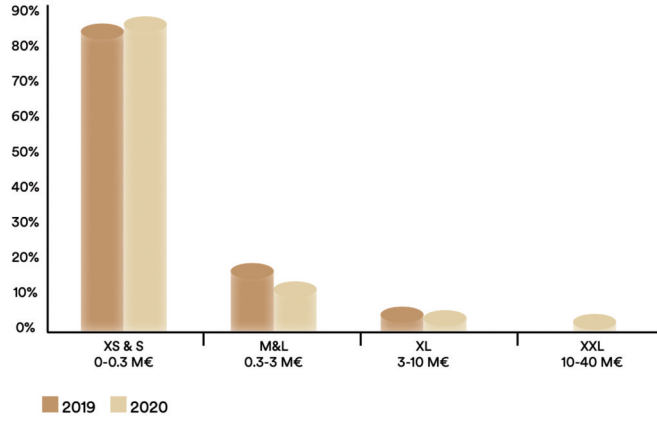


Figure 2: Proportion of claims in each segment
(source: LUCY study by AMRAE in 2021)



Another approach is to analyse in more detail the causes that weigh down the distribution tail. Roughly speaking, our inability to manage a risk is of course linked to its severity, but it is also partly linked to our ignorance. Indeed, cyber losses are extremely heterogeneous in nature. They vary in terms of their modus operandi (ransomware, denial of service attacks, etc.), their consequences (loss of business, theft of personal data, etc.), and the nature (sector exposed to the media or not, etc.) and behaviour of the victims (negligence, good computer hygiene, etc.). The distribution of losses therefore reflects this heterogeneity.

The problem is that statistical analysis of this tail index, which is so essential in understanding severe losses, tends to be aligned with the worst case scenario. Thus, taken separately, two categories of claims can have different tail indices (one low, and the other close to 1, which is the critical value). Taken together, without distinguishing between them, statistical estimation methods will align themselves with the heavier tail, and will eclipse the part corresponding to smaller claims that could be more easily managed if treated differently. This effect can be significantly mitigated by the numbers in each of these categories, but remains salient over large volumes of data.

If the analysis of these two categories is not differentiated, there is a danger that a certain type of claims (or policyholders) will be penalised too heavily. In addition to the understandable dissatisfaction of clients, this can lead to a disinclination to take out insurance, thereby reinforcing the imbalance in the system. Hence the need for a fine-grained analysis of the risk factors affecting the distribution tail, in order to efficiently classify policyholders and claim types. In [FTL21] we propose methodologies combining machine learning and extreme value theory that can be used for better classification of cyber events. This methodology is not unique, and other methods, often termed tail index regression, have been proposed in the literature (see for example [BGS+06]), each with their advantages and disadvantages.

In any case, these analysis methods are promising because they make it possible to identify the most sensitive cases. Based on this understanding of risk, strategies for optimising the scope of the insurance contract can be devised: for example, making the benefits of moderate risks more attractive so as to increase the volume of the portfolio and thus mutualisation.

Figure 4 in Box 4 shows the type of classification that can be obtained from the methodology proposed by [FTL21]. Starting with a population deemed to be “uninsurable” (because its tail index is greater than 1), a detailed study shows that a large majority of the situations considered are in fact associated with a tail index lower than 1 (82%), while only a small proportion (18%) is uninsurable or requires greater constraints to become insurable.

To achieve this level of analysis, however, it is essential to have sufficient information for the analysis of the most important risk factors.

Box 2: Mutualisation

Mutualisation is at the heart of the insurance business. If the insurer were to sell only one contract, the insurance operation would amount to a gamble, with potentially a very large loss in the event of a claim by the policyholder. The insurer must therefore try to bring together a large number of homogeneous and independent policyholders and carry out a mutualisation operation: the premiums received from all the policyholders will be available to compensate those who experienced a claim.

This principle of mutualisation is based on the mathematical theorem of the (strong) Law of Large Numbers (LLN).

Statement of LLN: Let (X_i) be a sequence of independent and identically distributed random variables with finite expectation noted m. Then, when n tends to infinity, the empirical mean $\frac{1}{n}\sum_{i=1}^{n} X_i$ converges (almost surely) to $m = E(X_1)$.

Applied in an insurance context, the law of large numbers means that, even though the claim amount X_i(or indemnity) for each policyholder i is random, when damage is identically and independently distributed, the average claim amount per policyholder is in fact almost constant and therefore 'predictable', and approximately equal to the mathematical expectation of the indemnity. This makes it possible to determine a "pure premium" for the insurance contract.

Furthermore, the larger the number of policyholders, the more accurately the average cost of insurance per individual can be predicted. The Central Limit Theorem (CLT) therefore allows the difference between the total charge and the earned premium to be controlled.

Statement of CLT: Let (X_i) be a sequence of independent and identically distributed random variables of finite expectation and variance denoted m and σ^2. Then when n tends to infinity,

$$P(|\sum_{i=1}^{n} X_i - nm| \leq \sigma\sqrt{n}\, q) \to \frac{1}{2\pi}\int_{-q}^{q} \exp(-x^2/2)dx$$

Thus, if the risks are independent and identically distributed and of finite variance, then the distribution of the total charge is asymptotically Gaussian.

Box 3: Extreme Value Theory

Extreme Value Theory provides a classification of probability distributions according to their distribution tail. In particular, it provides a theoretical framework which ensures that the distribution tail (i.e. the probability law of the largest values taken by a random variable) can be approximated and extrapolated through a simple law. This extrapolation is particularly suitable for so-called "heavy-tailed" phenomena such as those encountered in the field of cyber-risk. In this box, we provide some introductory information on this subject.

The Fisher, Tippett and Gnedenko theorem (see [BGS+06]) is concerned with the law of the maximum of a sample of identically distributed independent variables $(X_1,...,X_n)$. If we denote M_n this maximum, the result shows that the distribution of this quantity (properly centred and normalised) can only belong to a restricted set of probability laws (GEV, for Generalized Extreme Value distribution). These distributions are those of variables Z whose survival function is expressed as $H_\gamma(z) = \mathbb{P}(Z \geq z) = \exp(-(1+\gamma z)^{-1/\gamma})$ when $1+\gamma z > 0$ and $\gamma \neq 0$ (or $H_\gamma(z) = exp(-exp(-z))$ in the case where $\gamma = 0$).

The parameter γ (tail index) becomes a way of characterising the distribution of the largest values taken by the variables X_i : these variables are said to be in the domain of attraction of H_γ.

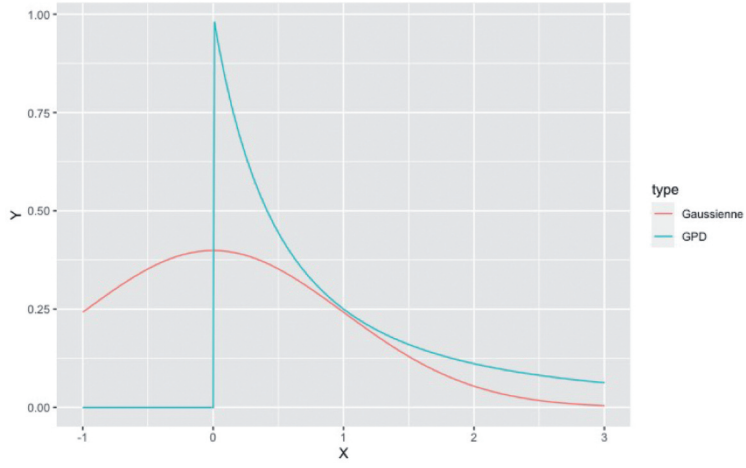
In the case of particularly volatile phenomena, such as the cost of a cyber claim, which can take on values very far from the average cost with a significant probability, we are faced with a strictly positive value of γ. The greater the value of γ the more the variable will tend to take very large values. Thus, if $\gamma \geq 1/2$, variance, traditionally used to quantify the "chaos" contained in a random phenomenon, becomes infinite. If $\gamma > 1$, it is the notion of average value that is jeopardised, since the expectation of the random variable becomes infinite. In this case, we sometimes speak of an uninsurable risk, since pricing is based on an equalisation of the expectation of the commitments of the two parties (insurer and insured).

A Pickands theorem further ensures that, if $\gamma > 0$, the tail distribution of the phenomenon can be approximated by a generalized Pareto distribution. Mathematically, if we introduce $S_u(x) = \mathbb{P}(X - u \geq x | X \geq u)$ i.e. the excess distribution function (the law of $X - u$ conditional on $X \geq u$), we have $\lim_{u \to \infty} \sup_{x>0} |S_u(x) - G_{\gamma,\sigma(u)}(x)| = 0$, for some function $\sigma(u) > 0$,

and where $G_{\gamma,\sigma}(x) = \frac{1}{\left(1+\frac{x\gamma}{\sigma}\right)^{1/\gamma}}$ is the survival function of a generalized Pareto law.

This result is particularly interesting if one wishes to model the distribution tail of the random variable, and in particular to anticipate particularly high values that it could take. Statistically, we will try to identify among the observations a threshold u from which the generalized Pareto approximation seems reasonable. This choice is the result of a compromise. On the one hand, u must be large enough for the generalized Pareto approximation to be legitimate; on the other, it must be small enough for a significant number of observations in our sample to be above this threshold. These observations exceeding u will be used to estimate the parameters γ et σ ,and their number will determine the quality of the estimate.

Figure 3: Graphical comparison of the probability density of a Gaussian distribution and a generalized Pareto distribution

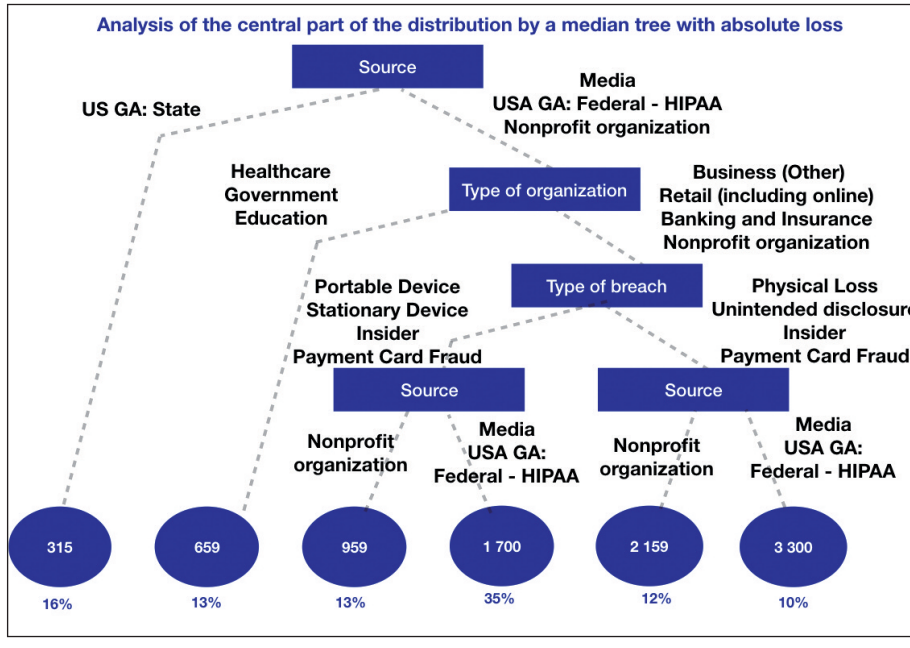


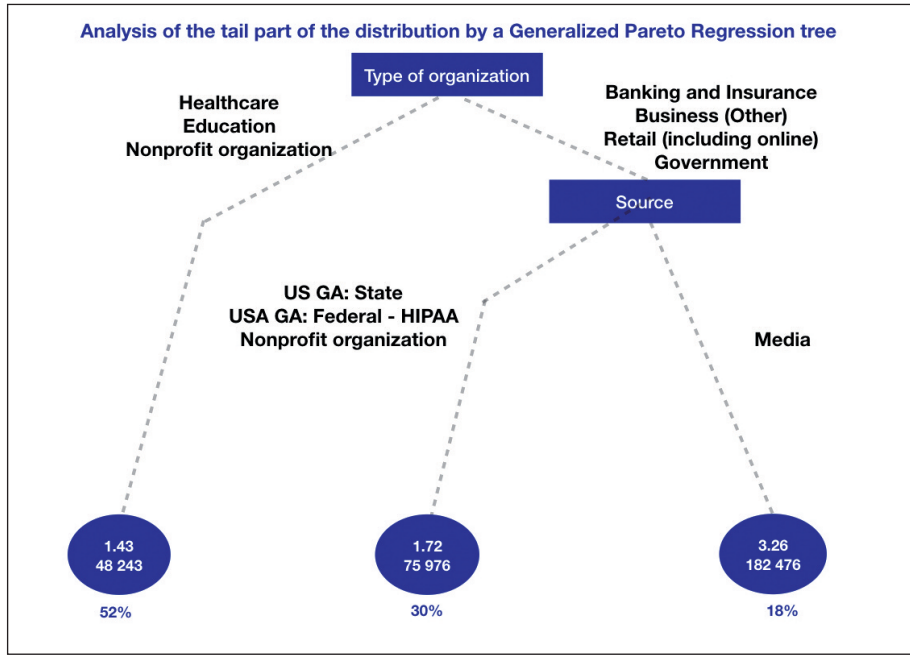
Note the slow decay of the generalized Pareto density, a symptom of the explosive nature of the distribution (large values can be taken with a relatively high probability).

Box 4: Classification trees

Figure 4 below shows two regression trees obtained by analysing the PRC database (see Box 5), that records data leaks. Each node in the tree corresponds to a characteristic variable of the leakage, such as the type of organisation that was breached (see [FTL21] for a full list of characteristics). Depending on the value of this characteristic, the corresponding left or right branch is explored. The leaves of the tree (at the bottom of each figure) represent the risk classes thus obtained. The first tree corresponds to an analysis of the central part of the distribution, i.e. it highlights the determining factors concerning the severity (here expressed in the volume of lost data) of a standard cyber event. The second tree provides a classification in terms of the distribution tail: each leaf of the tree represents a class of claims associated with a different value of the parameter γ, the first number in the bubble, and σ, the second number (see Box 3 for the definition of these parameters). [FTL21] shows the geometric disparity between these two graphs, indicating that the determinants of a typical loss are different from those of a severe event. Note that the authors identify a threshold of γ equal to 2 (pertaining to the distribution of the volume of data lost and not to the amount of the loss), above which the category of incidents is considered uninsurable. The tree on the bottom shows that 82% of the cases correspond to a γ smaller than 2, while only 18% appear critical. Furthermore, [FTL21] shows that an analysis of these data without distinguishing between the different types of events leads to the conclusion that they are globally uninsurable.

Figure 4: Classification trees obtained in [FTL21] using PRC data





III. Systemic components

Among the many characteristics of cyber events, those related to their systemic nature and self-exciting behaviour are of major importance. This systemic component of cyber risk is exacerbated by the fact that most information systems have similar vulnerabilities and are interconnected.

3.1. Auto-correlation and clustering of cyber events: modelling by multivariate Hawkes processes

In this context, modelling the frequency of cyber-attacks involves consideration of complex dependency effects. Standard actuarial models use the Poisson process to model the frequency component of risk. This Poisson model is based on the assumption that claims arrive independently of each other, and therefore appears to be unable to take into account the auto-correlation between cyber events and clustering effects. These auto-correlation phenomena are illustrated in Figure 5, which represents the auto-correlations of data breach events recorded in the Privacy Rights Clearinghouse [PRC] database, see Box 5.

We find that the arrival dates of events are not independent (the points are not uniformly distributed in the windows), and auto-correlation increases significantly if we focus on attacks of the same type or sector. Moreover, a Kolmogorov-Smirnov test (cf. [F62]) refutes the exponential distribution hypothesis for the inter-event times, with a p-value close to zero[2]. Hence the need to use dynamic models in which the arrival intensity of events (also called the hazard rate) is stochastic.

The alternative proposed in [BBH20] is based on multivariate Hawkes models, which are able to capture the self-excitation and interactions of cyber-events according to their characteristics, while benefiting from an interpretable and relatively parsimonious parametric representation. Hawkes processes are counting processes whose intensity is entirely specified by the process itself (see Box 6 and Figure 6).

Several excitation functions ϕ can be used, the exponential function being the most common (as it allows explicit calculations, thanks to the Markovian structure of the intensity in this framework). But other kernels, especially with a time delay, sometimes fit the data better (as is the case with PRC data, see [BBH20]).

First introduced by Hawkes [H71] and subsequently used in seismology to model earthquake aftershocks, they have since then been widely applied to many different areas, including finance, neurology, population dynamics or social network modelling, in particular because of their ability to translate excitation effects. In relation to cyber-risk, one of the first studies was carried out by Baldwin and his co-authors [BGI+17], underlining the

[2] When a hypothesis test is conducted, it is based on the calculation of an indicator from the sample (known as a statistical test). The value of this statistical test is compared to a threshold that determines whether or not the null hypothesis – called the null hypothesis – should be rejected. The threshold depends on the statistician's degree of "prudence" (the test level). A low p-value (close to 0) means that any statistician using a "reasonable" level will reject the null hypothesis.

relevance of Hawkes processes for modelling the occurrence of cyber-attacks in information systems, as these processes capture both the shocks and their post-shock persistence, which can result in a contagion of attacks.

This self-exciting behaviour leads to the clustering phenomenon and auto-correlation of cyber event arrivals.

Given the heterogeneity of cyber risk, types of attacks and their targets, [BBH20] proposes modelling using multivariate Hawkes processes: each event increases the probability of occurrence of a new event, within the same group/sector or type of attack (self-excitation), and each event within a group potentially increases the probability of occurrence of a new event within another group (inter-excitation). A penalised inference procedure can then be developed to capture the relevant interactions between the different classes of events and predict the joint distribution of the number of attacks according to their characteristics, as in [BBH20].

This procedure is the first step in quantifying the frequency component of cyber risk. However, to fully capture the frequency component, it would also be necessary to have information on exposure, which is very difficult to obtain from public databases such as the PRC. For what part of the variation over time in reported claims is caused by a change in the risk, and what part is caused by instability in the way the data is collected? In order to determine exposure, it is necessary to track the number of entities exposed to cyber risk over time, while ensuring the comprehensiveness of the claims reporting process within public databases, enriched with data from insurers, who have greater expertise than public databases regarding exposure, although less regarding losses.

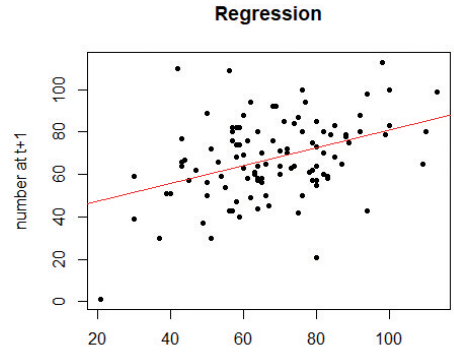
Box 5: The Privacy Rights Clearinghouse (PRC) database

The Privacy Rights Clearinghouse (PRC) database is a public database of data breaches targeting U.S. industry. It records various characteristics such as the name of the targeted entity, its sector of business, its location, the date of the breach report, the type of breach, the number of people affected, the source of information that reported the data breach to the database (U.S. government agencies, non-profit organisations, the media, etc.). An indication of severity is also given through the volume of data breached, which is useful for insurance applications.

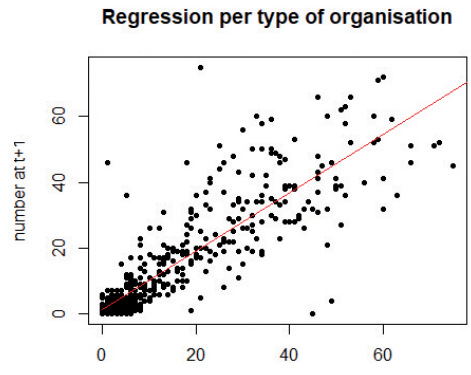
This database has been used in several academic studies on cyber risk, such as [MS10], [FHE16], [EL17], [FLT21]. However, it is not fed by an insurance portfolio but by various sources of information, each of them reporting heterogeneous types of claims. In particular, exposure, i.e. the number of entities exposed to risk within the PRC organisation, is unclear. Thus the PRC public database should be regarded with caution. It is used here primarily to illustrate our methodology, which can easily be extended to other types of data.

Figure 5: Regression of the number of events in month t+1 against the number of events in month t

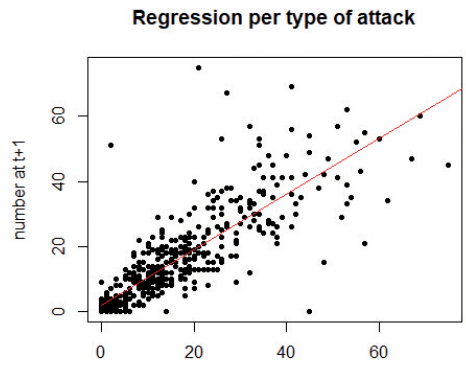
(PRC Database - Period 2010-2018)



R^2 = 0.164, Confidence Interval (95%) [0.030, 0.278]



R^2=0.780, Confidence Interval (95%) [0.750, 0.810]



R^2=0.726, Confidence Interval (95%) [0.687, 0.766]

Box 6: Point processes and intensity

Let $N_t = \sum_{n>1} 1_{T_n \leq t}$ be a point process where T_n is the time of the n-th jump, characterised by its jump intensity (also called hazard rate) λ_t : Intensity λ_t represents the "probability" of having a jump at time t, given past information.

1. N_t is a homogeneous Poisson process, with a positive constant jump intensity λ, if the inter-jump times $(T_n - T_{n-1})$ are independent random variables with the same exponential law of parameter λ : $P(T_n - T_{n-1} > t) = exp(-\lambda t)$

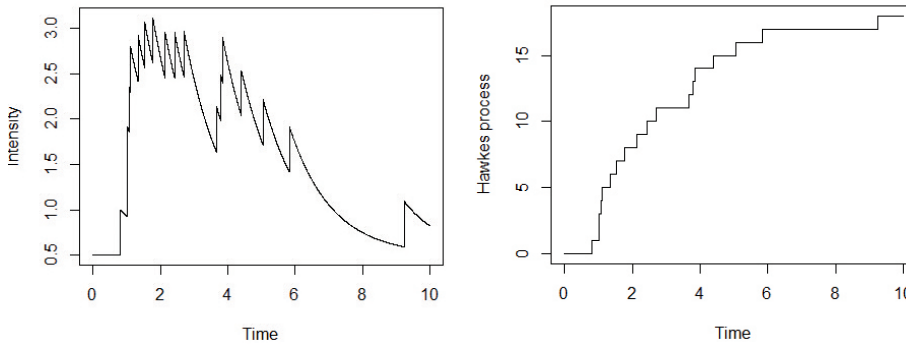
2. N_t is a non-homogeneous Poisson process, characterized by a deterministic (positive) intensity λ_t if the inter-jump times $(T_n - T_{n-1})$ are independent, with a distribution given by $P(T_n - T_{n-1} > t) = exp\left(-\int_0^t \lambda_s ds\right)$

3. N_t a Hawkes process with excitation function ϕ (positive deterministic function) and is characterised by a stochastic intensity λ_t defined by $\lambda_t = \mu_t + \sum_{T_n<t} \phi(t - T_n)$ with μ_t a (positive) deterministic function.

For a Hawkes process, the intensity λ_t is therefore characterised by a reference intensity μ_t which represents the rate at which a jump occurs "spontaneously", plus a self-excitation component $\sum_{T_n<t} \phi(t - T_n)$ where ϕ is the excitation function (or kernel) of the Hawkes process, which reflects the fact that past jumps also influence the occurrence of a jump at date t.

Figure 6: Trajectory of a univariate Hawkes process and its corresponding intensity process

Each jump represents an event. The excitation kernel used here is the exponential function $\phi(s) = \alpha exp(-\beta s)$: it is clearly observed that the intensity decreases exponentially between jumps.



3.2. Accumulation risk for cyber losses

The systemic potential of cyber risk is also based on the possibility of a simultaneous outage of a very high proportion of policyholders. A report by Cyence and Lloyd's of London [L17], for example, estimated that, if a loss occurred at a cloud provider, the cost of the attack would be in the range of 15 to 121 billion dollars, with an estimated average loss of 53 billion dollars. An example of such a massive cyber-attack is the Wannacry ransomware attack in May 2017, which led to the contagion of about 300,000 computers in more than 150 countries (see Box 1). It is important to note that even if the cost of each individual incident is low, the simultaneous occurrence of a large number of incidents in a massive attack can result in very high cumulative costs. These types of crises, called "accumulation scenarios", can undermine the principle of mutualisation, which is at the heart of the insurance business. Indeed, in these situations, the assumed independence of the insured parties, which is the central assumption of the Law of Large Numbers and which underlies the principle of mutualisation, is no longer valid (see Box 2).

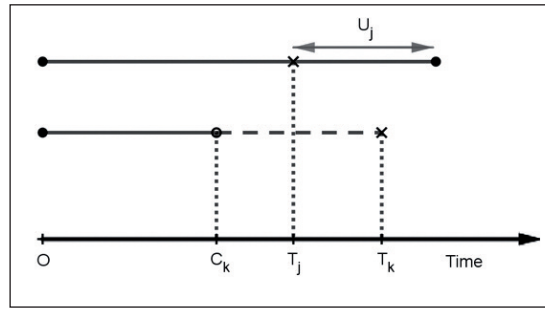
Moreover, if a large number of policyholders are simultaneously victims of an attack, the insurer's response capacity may become saturated. Indeed, in addition to financial compensation, cyber policies generally include more unusual services for the sector, since they are coupled with the provision of prevention and assistance in the event of a loss (by teams of experts such as cyber security firms) to help the insured party recover. This assistance has to be rapid and highly reactive, in order to avoid aggravating the damage. The inability of the insurer to intervene appropriately within a short timeframe can lead to additional losses, such as financial penalties and loss of reputation, as well as further damage for the insured, who becomes stranded with no assistance. To meet these commitments, the insurer must therefore be able to anticipate the level of response required during such a crisis.

The design of accumulation scenarios is therefore a real challenge for the insurability of cyber risk, with a view to anticipating the impact of a massive cyber-attack on an insurance portfolio and assessing its resilience. [HL21] proposes a general and flexible methodology that can help insurance companies design their strategies against such cyber storms and to determine the response capacity (in terms of prevention and reaction time to the attack).

The construction of these accumulation scenarios in [HL21] is based on stochastic epidemiological contagion models adapted to the context of cyber risk, similar to the virus contagion models, like those used for the Covid-19 pandemic. Barrier measures, such as vaccination, are replaced here by other preventive measures, such as identifying and correcting vulnerabilities. And the risk of the saturation of intensive care services is replaced by the risk of being unable to provide all the necessary assistance to the insured. Nevertheless, despite the analogy between cyber and biological epidemics, there are still differences, particularly in terms of time scales, parameter values and the nature of the risk. Consequently, the existing models need to be adapted to the cyber context.

In order to ensure flexibility, the modelling process is divided into three separate parts (see Box 7).

Box 7: Micro-modelling of the cyber-epidemic: chronology of events for policyholders j and k



For a given policyholder, we define:

T = date when the policyholder is infected (can be $+\infty$),

U = duration of assistance after infection,

C = time after which the policyholder applies a remedy that prevents infection.

1. **The "environment" module**, corresponding to the modelling of the random variable T, i.e. the severity of the infection in the global population.
2. **The "repair" module**: modelling the random variable U, which represents the immediate intervention time to "provide first aid", and depends on the type of infection modelled (ransomware, data corruption. etc.).
3. **The "prevention and response" module**: modelling the random variable C, which represents the reactivity of the actors in detecting the threat and responding to it.

For the environment module, a compartmental model of the SIR type (susceptible, infected, cured or recovered) can be used (see Figure 7). This is characterised by two parameters: the infection rate denoted β, and the recovery rate denoted γ. The reproduction number $R_0 = \beta / \gamma$ characterises the virulence of the epidemic: if $R_0 < 1$ the attack is extinguished, and if $R_0 > 1$ it spreads. The "cured" in this context are policyholders who no longer need assistance in the short term, and thus no longer contribute to the saturation of the insurer's response. A "full" cure can take much longer.

The amounts S, I and R of the three compartments satisfy the system of differential equations.

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

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

$$\frac{dR(t)}{dt} = \gamma I(t).$$

We have chosen to present here the SIR epidemiological contagion model. Although this is intended to be simple, network effects in particular are absent, or at least not obvious, since they are diluted in a collective macro view of the cyber-epidemic. Network structures can of course have a significant impact on cyber risk losses. To capture these, we can replace, for example, the SIR model with a multi-group SIR model in which policyholders are separated into different categories. The links between the different categories can vary in strength, thus giving rise to a matrix of coefficients whose values represent the network: more connected categories are associated with higher contagion parameters. It is, moreover, possible to model non-contagious attacks, since a homogeneous attack rate can also be used to model the random variable T, corresponding to certain event patterns, such as some massive spam campaigns. Nevertheless, it must be emphasised that it is difficult to calibrate cyber-attack scenarios, especially as information on network structures is almost impossible to obtain, especially for small companies.

As soon as the threat has been detected (e.g. after a delay of a few days) and remedies are identified, policyholders can implement them. Different reaction dynamics over time can be considered: for example, a constant implementation rate (corresponding to an exponential distribution), a decreasing implementation rate (Pareto distribution), or an increasing implementation rate (Weibull distribution), (see Figure 8).

Once the three modules have been implemented, various risk monitoring indicators can be analysed, having first adjusted the parameters of the epidemiological model to the kinetics of Wannacry, see [HL21]. For example, Figure 9 represents, for 10,000 scenarios, the evolution over time of the number of victims during a Wannacry-type cyber-attack as a function of the speed of the response and the form taken by the countermeasures implemented. We can thus visualise the reduction in the peak as a function of behaviour. As can be seen, what matters is not so much the form of the response, but above all its speed, which is crucial for reducing the risk of saturation: a slow response will barely reduce the load on the support teams (a reduction of only about 4%), whereas a rapid response within three days considerably reduces (by up to 30%) the peak in the number of policyholders requiring support. Nevertheless, even a slower response will still have a beneficial effect on the total number of victims.

In conclusion, the framework for constructing accumulation scenarios presented here is flexible and can easily be generalized to any other type of model for the dynamics of the attack and the quality of the provider's intervention (the duration of recovery), or to represent the behaviour of policyholders with regard to prevention. For example, the dynamics of the epidemic, i.e. the contagion model, can be easily enriched if one wishes to introduce network effects, reflecting greater contagion between certain activity sectors that are more connected than others. Furthermore, particular attention must be paid to the definition of realistic global scenarios for describing such a cyber-epidemic. At the moment, there is a lack of public data to clearly identify the precise chronology of massive cyber-attacks. The example used here, inspired by the Wannacry crisis, should only be viewed as a rough guide, due to the number of assumptions made in our attempt to replicate this episode.

Figure 7: SIR epidemiological model

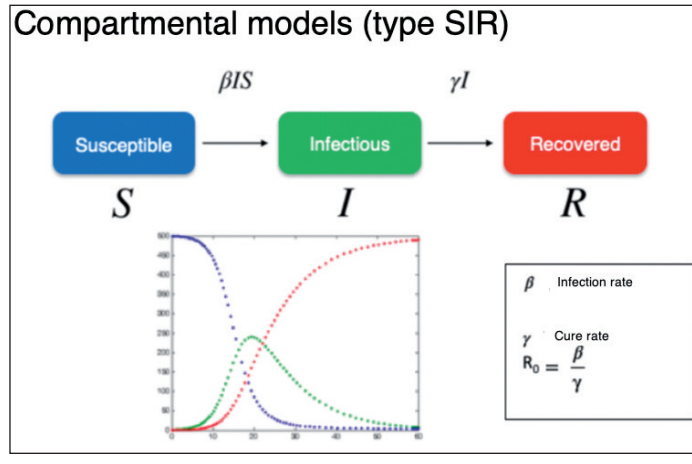


Figure 8: Different dynamics of implementation rates of protective measures

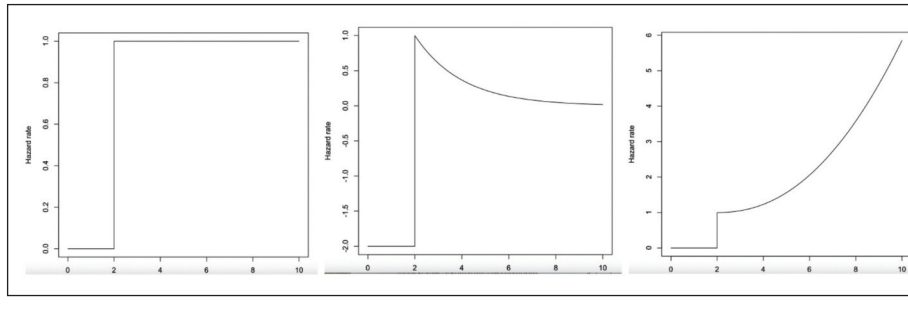
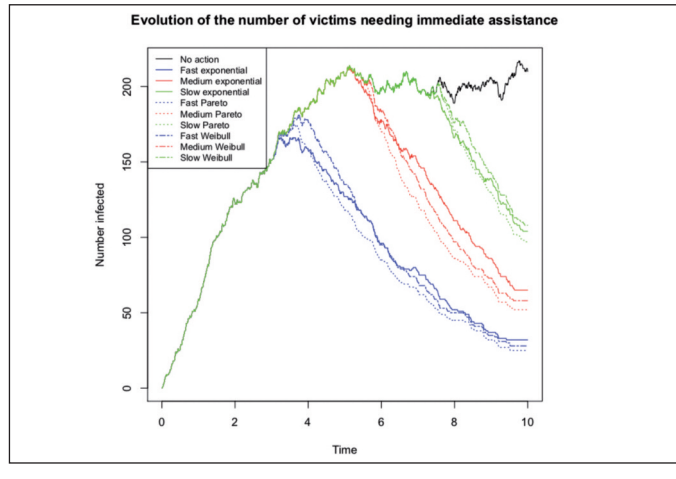


Figure 9: Evolution over time of the number of victims in need of assistance



IV Databases, and behavioural characteristics of victims and malicious actors

4.1. Creating a cyber risk observatory

There are few public data sources that allow real-time monitoring of cyber risk. GIP Acyma, through its cybermalveillance.gouv.fr platform, collects and produces statistics that make it possible, through its publications and activity reports, to obtain quantitative information on the evolution of the threat. This is also the case with ANSSI publications, including the report on ransomware [ANSSI21b]. AMRAE, in its study "Light upon cyber insurance" (known as "LUCY") [LUCY21] has produced, via a survey of brokers, a sizable inventory of claims encountered by insurers. The output of these different data sources is extremely valuable for quantifying cyber risk on a variety of scales.

However, these statistics are not yet mature enough to provide a comprehensive view of the risk and to react quickly to its evolution.

By lack of maturity, we mean either the absence of very precise information on the risk, or the imprecision of the collection methods and their stability over time, which if remedied would make it possible to ensure the reliability of the data and its monitoring over time. To take the example of the ANSSI report on ransomware, a lot of potentially valuable information on the scale of attacks comes from poorly specified sources, some of which is taken from reports by cyber security companies whose methodology for producing statistics is opaque. Another telling example concerns the study of the proceeds generated by ransomware (see [ANSSI21b]). The amounts estimated are sometimes subject to a large margin of error, as in the case of Cryptowall, where the losses generated are put between 18 and 320 million dollars. It is not so much the magnitude of this margin of error that raises questions – it is quite understandable given the complex evaluation of the profits of criminal organisations, including clandestine ones – as the source of this information, about which little is known. This lack of information is of course explained by the extremely sensitive nature of the material, but it complicates the assessment of the risk.

Moreover, cyber risk is evolving extremely rapidly. A good example is provided by the increase in the number of cyber-attacks in the first few months of 2021. However, these statistics were not updated as rapidly as they are today.

In order to better identify what is currently missing in the cyber sector, it is interesting to compare it with another type of threat, which concerns health monitoring. The choice of the parallel is significant. The very term 'computer virus' immediately suggests an analogy between biological epidemics and the functioning of cyber infections. Moreover, epidemiology is a field where the reliability of data cannot be taken for granted. In monitoring a biological virus, the tools and methods for recording cases are not necessarily available. Diagnostic errors can also introduce errors.

The Sentinelles network (see https://websenti.u707.jussieu.fr/sentiweb/) provides an example of a statistical tool for recording and monitoring data related to a changing threat that is highly dependent on human behaviour. Through weekly public reports, the network monitors acute respiratory infections (influenza before the outbreak of Covid-19), acute diarrhoea, and chickenpox. Other pathological indicators are also recorded, as part of the Santé Publique France surveillance systems.

Underlying initiatives such as Sentinelles, which was launched in 1984, there is a whole culture and expertise in public health data that proves extremely valuable in the event of a crisis. For example, between 1987 and 2002, the tool was adapted to include valuable information on HIV tests that were not initially included among the infections targeted. Throughout the Covid-19 epidemic, the public data transmitted daily by Santé Publique France (available on https://dashboard.covid19.data.gouv.fr/vue-d-ensemble?location=FRA) has very much benefited from this experience, and has been characterised by exemplary rigour in view of the complexity of the problem. Of note in particular is the systematic documentation accompanying each publication of data, and the transparent rectification, if necessary, of any errors observed in some retrievals.

This level of information is currently lacking in the monitoring of the cyber threat and the prediction of its evolution. It should be remembered that, in the field of cyber insurance, forecasting is crucial, since pricing and provisioning are based on predicted future costs. Furthermore, prevention, a key aspect of threat reduction, would benefit greatly from a real-time barometer, especially since the time scale of cyber risk is quite short.

Computer security companies provide various real-time measures (see in particular Kaspersky, https://cybermap.kaspersky.com/), but making use of them is difficult due to the problem of quantifying their biases and the lack of precise documentation on their methodology.

4.2. Behavioural aspects

In its 2020 activity report, Cybermalveillance [ANSSI21a] describes the Covid-19 crisis as a “windfall” for cyber criminals. As soon as the first lockdown measures were introduced in Europe, there was a significant increase in cyber threats related to the disease (see [LSN21+]): by April 2020, a significant number of malicious sites or fraudulent emails were attempting to exploit the epidemic. In addition, there was a massive and not always anticipated shift to working from home, leading to the insecure use of personal digital tools in a professional context, thereby increasing vulnerability, see [BS20]. Health-related attacks also proliferated, including the one against the European Medicines Agency (see https://www.ema.europa.eu/en/news/cyberattack-ema-update-5) with regard to the validation of vaccines. Although health institutions are typically highly exposed (the NHS was one of the most publicised victims of the Wannacry cyber-attack in 2017 [GKH+19]), the Covid-19 situation, by making them the focus of attention, may partly explain the increase in these attacks.

This example of the Covid-19 crisis illustrates one of the most worrying characteristics of cyber-risk: the great adaptability of hackers and their remarkable opportunism. Thus, although the term ‘cyber-hurricane’ (used for example by the Institut Montaigne in its report

[M18]) is often used to describe the catastrophic dimension of the risk, this disaster is by no means a natural phenomenon.

Indeed it is a human risk, requiring a better understanding of the behaviour of the actors. In insurance, the importance of policyholder behaviour is well known. The phenomena of anti-selection and moral hazard (see [P78]) are important issues in insurance econometrics. Anti-selection relates to behaviour prior to taking out insurance: for someone to begin the process of becoming insured, he/she must be more sensitive to risk, and therefore more exposed than an average individual in the population at large. Moral hazard, on the other hand, reflects a change in behaviour after the policy is taken out: policyholders who consider themselves to be protected by their contract may adopt a less prudent attitude. Conversely, the insurer, in taking on the risk, wagers on the virtuous behaviour of the client for limiting any losses.

With regard to natural hazards, prevention yields valuable insights in terms of risk reduction, see [P18]. Transposing this model to the cyber context seems essential. Nevertheless, the extreme adaptability of cyber criminals gives rise to fears of the greater instability of the threat. In the case of natural risks, changes have of course been observed, particularly in relation to climate change, but however worrying they are, these changes are expected to occur over a longer time frame than in the case of cyber crime. Thus the 255% increase in ransomware attacks in 2020 reported by [ANSSI21a] occurred very suddenly. Therefore in order to understand and anticipate such events, there needs to be a better understanding of the attackers and their operating methods.

4.3. Ways of operating

The Cybermalveillance 2020 activity report [ANSSI21a] provides some indicators on the main types of attacks that have been reported to the platform. Phishing (representing 17% of reports to Cybermalveillance) appears to be the main vector, reflecting once again the importance of the victims' behaviour: by clicking on a fraudulent link, the victim makes the attack possible. But this threat is difficult to distinguish (as the authors of the report mention) from the second category, namely "account hacking", which can be caused by phishing (typically, victims transmit Their identifiers following a response to a fraudulent e-mail). This difficulty in accurately classifying incidents is an obstacle to the effective use of statistics on the subject.

It is interesting to note in the Cybermalveillance figures that "webcam blackmail" accounts for a significant proportion of reports (around 8%). This phenomenon, particularly publicised through the so-called "Cryptoporno" case (see https://www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/chantage-a-lordinateur-ou-a-la-webcam-pretendus-pirates) requires a very low level of technology on the part of the attacker. It is a classic scam, in which the criminal pretends to have hacked the victim's webcam and blackmails him, threatening to publish compromising videos if he does not comply. The success of the scam relies mainly on the credulity of the target, as the webcam has not necessarily been hacked.

This type of incident mainly affects private individuals, who are not currently the core target of cyber insurance products, which are geared towards businesses. Nevertheless, it is important to pay attention to them because they reveal the effectiveness of low-tech attack methods. Companies can also be hit by scams that could be described as traditional, in

that they existed before the computer age, but have been transposed into a digital framework. A good example is the “president fraud”, which typically involves identity theft where a criminal poses as a senior company official and obtains a fraudulent transfer. This is more manipulation than hacking, even if the digital medium is used.

Social engineering also plays an important role in so-called “Big Game Hunting”. This type of large-scale attack, described in particular in the ANSSI report on ransomware [ANSSI21b], requires considerable preparation on the part of hackers. Several vectors are used to infiltrate the company (digitally, but sometimes physically) in order to generate maximum damage, forcing the victim to pay the ransom. The ransomware attack can also be reinforced by denial of service attacks that can paralyse part of the network.

While this type of large-scale digital heist requires a high degree of professionalism on the part of the criminals, not all attacks are of this nature. The emergence of ‘Ransomware as a Service’ (RaaS) (see [MBS20]) makes hacking kits available to malicious individuals, who can then cause damage without requiring a high level of computer literacy.

4.4. Cybercrime actors

The ‘Ransomware as a Service’ phenomenon also reveals the importance of the business model on which the cyber-criminal ecosystem thrives. In 2017, Wannacry [MP17] generated several hundred million dollars in losses, but the ransom amounted to barely 100,000 euros (see https://github.com/rwillmann/WannaCry-Outbreak-Data-12-May-2017---19-May-2017), this amount being known because the transactions on the bitcoin addresses concerned are publicly available. Through RaaS, criminals have devised a subscription system, with users paying royalties to the authors. This allows some ransomware to generate much larger profits over a long period of time: an estimated 6 million dollars for SamSam between 2016 and 2018, between 7.8 and 150 million for Locky between 2016 and 2018, and 150 million for GandCrab between 2018 and 2019.

Moreover, some actors position themselves between criminals and their victims, thus flirting with illegality. The ANSSI report [ANSSI21a] refers, for example, to a company that offers to help the victim pay the ransom, and has concluded partnerships with certain hacker groups to obtain discounts on the ransom payment.

Greater understanding of these actors’ economic model is essential to foresee more clearly the evolution of the risk, and to counteract its implications. In the case of ransomware, objectively assessing the harmful impact of ransom payments on the proliferation of attacks would be a major contribution to defining a strategy to counter the evolution of this threat.

This is especially true given the complexity of the cyber-crime ecosystem and the fact that hackers’ motivations are not only economic. The NotPetya ransomware [F18], originally targeting Ukraine (Russia is suspected of being the perpetrator, (see https://www.lemonde.fr/pixels/article/2018/02/15/virus-informatique-notpetya-le-royaume-uni-accuse-la-russie-qui-dement_5257443_4408996.html), shows, if anything, the importance of geopolitics in cyber-attacks. Foreign intervention is also suspected of lying behind the massive attack on Australia in 2020 (https://www.lemonde.fr/international/article/2020/06/19/l-australie-se-dit-victime-d-une-cyberattaque-d-un-acteur-etatique_6043366_3210.html). Similarly the Solar Winds case [NYSDFS20] is believed to have been motivated by espionage.

In addition, there are ideological and non-financial motivations, sometimes referred to as cyber-hacktivism. Examples include the hacking of the Ashley Madison dating site in 2016 (see [MD15]) and the religiously motivated Operation Ababil (see [I13]).

These examples reveal a complex picture, with a certain porosity between the different types of cyber-criminals, as pointed out by the ANSSI [ANSSI21a]. As with climate change, where it is important to study the natural causes to predict how they will evolve, understanding this eco-system and its evolution is fundamental if we want to move from reaction to prevention.

V Conclusion

Faced with the inexorable rise in cyber risk, insurance appears to be an essential tool for increasing the resilience of the economic and industrial fabric against these attacks. But while the cyber-insurance market is developing – by putting forward innovative offers that combine prevention, financial compensation and support in the event of a crisis – it is becoming particularly stretched, in terms both of contract renewals and of insurance take-up by SMEs/ETIs, whose coverage rate is struggling to take off. This under-coverage poses risks to the companies and public authorities concerned, as well as to their entire ecosystem: subcontractors, suppliers, customers, commercial partners, etc.

In addition, many questions arise as to the viability of the cyber-insurance market, and the ability of the industry to pool losses in the event of a major disaster. Various factors jeopardise such mutualisation:

- The difficulty of quantifying, and therefore anticipating, the impacts of an emerging and rapidly changing risk.
- The shifting boundaries of the risk, particularly through “silent cyber”.
- The extreme volatility of damage from one cyber incident to another.
- The systemic nature of the risk, as a “cyber pandemic” may result in the simultaneous shut-down of many policyholders

With this level of uncertainty, constructing statistically reliable models requires a large amount of data. Without an extensive and reliable database, it is difficult to envisage an economic equilibrium where each company arrives at an assessment of risk based solely on its individual experience. Indeed, exploiting and exacerbating the existing imbalance is at the heart of the strategy of the malicious actors behind cyber incidents. Moreover, changing behaviours within the cyber eco-system (on the part of hackers, users, protection actors) prevents its rapid stabilisation. Faced with this uncertainty, the purely legal solution aiming to exclude certain types of events from contracts, and to introduce indemnity limits making cover less attractive, is not satisfactory. On the one hand, the objective of economic resilience becomes more difficult to achieve, and on the other, the impoverishment of cover hinders the development of the cyber insurance market, and, paradoxically, increases insurers’ risks by limiting their capacity for mutualisation.

Given this situation, we believe that information sharing is essential. Cyber risk is a fundamentally human risk, built on a contest between attackers (cyber criminals) and a society that seeks to protect itself while benefiting from the contributions of the digital revolution. In the context of this opposition, the attackers practise in their own way the sharing of information and know-how, pooling techniques, all the way up to turnkey packages in the framework of "Ransomware as a Service". The defenders' camp needs to catch up in terms of information exchange. The constitution of mutualised databases between cyber defence actors (insurers, public authorities, cyber security actors, etc.) seems to us to be essential for the creation of a viable economic model for insurance. The compartmentalisation of information – for example in the vain hope of gaining a competitive advantage – runs counter in our opinion to the urgent need for better quantification and collective anticipation of this risk.

REFERENCES

[ABT17] H. Albrecher, J. Beirlant, and L.T. Jozef. “Reinsurance: actuarial and statistical aspects”, *John Wiley & Sons*, 2017.

[ANSSI21a] Rapport d’activité 2020 de l’ANSSI
https://www.ssi.gouv.fr/agence/missions/rapport-dactivite-2020/

[ANSSI21b] Etats de la menace rançongiciel, ANSSI.
https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-001.pdf

[BBH20] Y. Bessy-Roland, A. Boumezoued and C. Hillairet. “Multivariate Hawkes process for cyber insurance”, *Annals of Actuarial Science,* 2020.

[BGI+17] A. Baldwin, I. Gheyas, C. Ioannidis, D. Pym, and J. Williams. “Contagion in cyber security attacks”. *Journal of the Operational Research Society, 68(07):780–791*, 2017.

[BGS+06] J. Beirlant, Y. Goegebeur, J. Segers and J. Teugels. “Statistics of extremes: theory and applications”. *John Wiley & Sons, 2006.*

[B20] E. Blosfield. “Cyber lessons for the insurance industry continue three years after NotPetya”. *Insurance Journal*, August 2020.
https://www.insurancejournal.com/news/national/2020/08/12/578788.htm

[BM09] J. Bolot and M. Lelarge. “Economic Incentives to Increase Security in the Internet: The Case for Insurance.” *IEEE INFOCOM 2009 p. 1494-1502.* 2009.

[BS20] D. J. Borkovich, and R. J. Skovira. “Working from home: Cybersecurity in the age of COVID-19.” *Issues in Information Systems* 21.4 2020.

[CEA21] Commissariat à l’Energie Atomique. “L’enjeu de la cybersécurité”. Les Défis du CEA N° 242 – Parution : Mars-Avril 2021

[CESIN] Club des Experts de la Sécurité de l’Information et du Numérique. “Baromètre de la cyber-sécurité des entreprises. Vague 6” – Janvier 2021 https://www.cesin.fr/publications-9.html

[CISA20] Cybersecurity and Infrastructure Security Agency’s (CISA’s).“Cost_of_Cyber_Incidents_Study”, Octobre 2020.
https://www.cisa.gov/sites/default/files/publications/CISA-OCE_Cost_of_Cyber_Incidents_Study-FINAL_508.pdf

[NYSDFS20] New-York State Department of Financial Services, “Report on the SolarWinds Cyber Espionage Attack and Institutions’ Response”, 2021, https://www.dfs.ny.gov/system/files/documents/2021/04/solarwinds_report_2021.pdf

[EL17] M. Eling and N. Loperfido, Data breaches: “Goodness of fit, pricing, and risk measurement.” *Insurance, Mathematics and Economics,* 2017.

[E21] P. Escande, AFP, “Etats-Unis : les oléoducs Colonial Pipeline ont versé une rançon de 4,4 millions de dollars à des hackeurs”, *Le Monde (ISSN 1950-6244)*, 19 mai 2021.

[EUROPOL18] Internet Organized Crime Threat Assessment (IOCTA) 2018, https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

[F18] S.Y.A. Fayi, “What petya/notpetya ransomware is and what its remidiations are” *Information technology new generations,* Springer 2018.

[FHE16] S. Forrest, S. Hofmeyr and B. Edwards. “Hype and heavy tails: A closer look at data breaches”. *Journal of Cybersecurity, 2(1):3–14*, 2016.

[FLT21] S. Farkas, O. Lopez and M. Thomas. “Cyber claim analysis through Generalized Pareto Regression Trees with applications to insurance pricing and reserving”*, Insurance: Mathematics and Economics,* 2021.

[F18] S. And Y. A. Fayi. “What Petya/NotPetya Ransomware Is and What Its Remidiations Are”. *In: Latifi S. (eds) Information Technology - New Generations. Advances in Intelligent Systems and Computing, vol 738. Springer, Cham.* 2018.

[F62] P. Ferignac. “Test de Kolmogorov-Smirnov sur la validite d’une fonction de distribution”. *Revue de statistique appliquée, tome 10, no 4 (1962), p. 13-32.* 1962.

[GKH+19] S. Ghafur, S. Kristensen, K. Honeyford, G. Martin, A. Darzi and P. Aylin, “A retrospective impact analysis of the WannaCry cyberattack on the NHS.” *NPJ digital medicine.* 2019.

[H71] A. G. Hawkes. “Spectra of some self-exciting and mutually exciting point processes.” *Biometrika, 58(1):83–90,* 1971.

[HL21] C. Hillairet and O. Lopez. “Propagation of cyber incidents in an insurance portfolio : counting processes combined with compartmental epidemiological models”, *Scandinavian Actuarial Journal,* 2021.

[I13] E. Iasiello, “Cyber attack: A dull tool to shape foreign policy”. *5th International Conference on Cyber Conflict (CYCON 2013)*. IEEE, 2013.

[LUCY21] Association pour le Management des Risques et des Assurances de l’Entreprise. “LUCY : LUmière sur la CYberassurance.” AMRAE, 2021 https://www.amrae.fr/bibliotheque-de-amrae/lucy-lumiere-sur-la-cyberassurance-amrae-mai-2021

[Lloyds17] Lloyds, Counting the cost – cyber-exposure decoded, *Cyence*, 2017.

[LP17] O. Lopez and F. Picard. “Cyber-assurance : nouveaux modèles pour quantifier l’impact économique des risques numériques”, *Revue d’économie financière*, 2019.

[LSN+21] H. S. Lallie, A. L. Shepherd, J. R.C. Nurse, A. Erola, G. Epiphaniou, C. Maple and X. Bellekens, “Cyber security in the age of COVID-19: A timeline and analysis of cybercrime and cyber-attacks during the pandemic,” *Computers & Security*, 2021.

[MBS20] P. H. Meland, Y. F. Fahmy Bayoumu and G. Sindre, “The Ransomware-as-a-Service economy within the darkness”, *Computers & Security*, 2020.

[MD15] S. Mansfield-Devine, “The Ashley Madison affair”, *Network Security*, 2015.

[MS10] T. Maillart and D. Sornette. “Heavy-tailed distribution of cyber-risks”. *The European Physical Journal B, 75(3):357–364,* 2010.

[MMN+15] A. Marotta, F. Martinelli, S. Nanni and A. Yautsiukhin.
“A survey on cyber-insurance.” *Bologna, Italy: Unipol Gruppo Finanziario SpA, 52*, 2015.

[MP17] S. Mohurle and M. Patil. “A brief study of Wannacry Threat: Ransomware Attack 2017”. *International Journal of Advanced Research in Computer Science, Volume 8, No. 5*, 2017.

[M18] Institut Montaigne. “Cyber menace : Avis de tempête”, 2018.https://www.institut-montaigne.org/publications/cybermenace-avis-de-tempete

[P18] P. Picard “Natural disaster insurance and the equity efficiency trade off”, *Journal of Risk and Insurance*, 2008.

[P78] M. V. Pauly, “Overinsurance and public provision of insurance: The roles of moral hazard and adverse selection.” *Uncertainty in Economics*. Academic Press, 1978.

[PRC] https://www.privacyrights.org/data-breaches

[RAK+19] S. Romanosky, L. Ablon, A. Kuehn and T. Jones
“Content analysis of cyber insurance policies: how do carriers price cyber risk?”
Journal of Cybersecurity, 2019.

[RM19] Etat de la menace numérique en 2019, https://www.interieur.gouv.fr/Actualites/Communiques/L-etat-de-la-menace-liee-au-numerique-en-2019

[T17] E. Tourny. “Cyber sécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya”. *Paix et sécurité européenne et internationale (7).* 2017.

Institut Louis Bachelier
Palais Brongniart
28, place de la Bourse
75002 Paris
Tél. : +33 (0)1 73 01 93 40
Fax : +33 (0)1 73 01 93 28
contact@institutlouisbachelier.org

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE DE L'ÉCONOMIE
DE L'INDUSTRIE ET DE L'EMPLOI

LABEX
Louis Bachelier

CONCEPTION GRAPHIQUE : VEGA CONSEIL 01 48 85 92 01