ASSOCIATION EUROPE FINANCES RÉGULATIONS

Debate Paper

Issue n° 2/2023 – January 2023

Insurability of large emerging risks

Author: Olivier Lopez

Professor at Sorbonne University, Director of the Institute of Statistics of Sorbonne Université (ISUP)

This Debate Paper[1] discusses how to take up the challenges triggered by the emergence and proliferation of large risks, which, if not properly mutualized, will undermine the social links that are fundamental to our society. To put together efficient risk transfer solutions, innovative mechanisms need to be developed. None of them constitute a miraculous solution, but a careful combination of them may improve prospects.

The goal is to achieve an efficient sharing of the risk among the various stakeholders: policyholders, State (taxpayers), and insurance companies. An appropriate combination of self-insurance and outside insurance should be finetuned, especially for large corporations. For households and small companies, harmonious collaboration between the public and the private sphere should be pursued. In some cases, State intervention is unavoidable; it should be anticipated and done with the idea of protecting both public finances and the economic stability of the private insurance sector; an active prevention strategy with all stakeholders (insurers but also policyholders) is key in that respect.

Given the extreme catastrophes linked to current developments, the issue of scale can only be solved at the European level, which has the proper dimension to face risks that do not acknowledge borders. In any case, all strategies that can be invented should be based on enough information to anticipate developments and organize financial protection. Collaboration in information sharing should be thought of as collaboration between European States. Aggregated data are not sufficient to make a precise analysis, which is essential for reducing uncertainty. The proper level of information is probably more to be found in the information stored by private actors (industries, insurance) than in national statistics. The public European sector could play a key role in organizing this information sharing between all the stakeholders concerned by risk, respecting privacy, competition, and defense.

The extreme severity of risk that we now face makes this effort of collaboration (within sectors and with the other forces concerned by risk) essential in extending the boundaries of insurability.

Introduction

The insurance landscape is undergoing considerable change due to the transformation of societies and global threats like climate change. The economic balance around the coverage of traditional risks, like natural

[1] This Debate Paper was prepared by a dedicated working group composed of representatives of institutional members of the AEFR participating in a personal capacity, whose aim is to initiate a discussion on key issues at stake regarding insurability of large emerging risks. The views expressed in this paper do not necessarily reflect the views of the individual members of the working group. The study has greatly benefited from interviews carried out with key institutional and market participating stakeholders, who should be thanked for their very valuable contributions.

disasters, has been disrupted by rapid changes in the physiognomy of risks that put into question the lessons of experience acquired by the market. In addition, new risks have emerged, like cyber, that make it necessary to learn how to develop strategies and procedures to manage them efficiently. The history of insurance is full of changes and evolutions of the social, technical and physical environment and constantly adapting to these modifications is one of the key features of this industry. What is particularly concerning in the present context is the propensity of these changes to lead to disasters, whose repeated magnitudes may exceed insurance capacities. This change in the risk environment raises the issue of the insurability of traditional risks as well as new ones.

Questioning the insurability of a risk may appear to be a false problem. Almost every risk can be insured, at least to some extent: deductibles, contractual limits on compensation, and exclusion clauses are technical ways to avoid endangering solvency. But this type of solution quickly reaches its limits, since it may leave policyholders holding a large share of the losses. The real challenge consists in developing mechanisms that allow insurance to endorse the major role it is meant to have in view of this new situation: offering, at a reasonable cost, financial reparation to help rebuild after an incident; enhancing the resilience of society.

The aim of this paper is to identify the levers that may help the sector to accomplish this mission, while being lucid about their limitations. Our approach is mainly economic, focusing on the necessity to properly quantify the cost (and the means to establish it) of the risk in an anticipatory perspective. The purpose is not to promote a specific solution: the response to such crucial challenges necessarily relies on the combination of several mechanisms (specific policies, prevention, reinsurance, public-private interactions…). We want to establish guidelines to design and to judge the viability of such a solution, and that may help to establish which part of a risk one may hope to cover with insurance.

We mostly consider three major risks that are of particular concern in the present context:

- natural disasters, with the evolutions caused by climate change;
- pandemics, in view of the current Covid-19 crisis and with the perspective of new threats that may rapidly spread in a globalized economy;
- cyber risk, in a context of extreme dependence by society on digital solutions and of the fear of systemic events whose impact is hard to anticipate.

The panorama that we propose does not pretend to be exhaustive, but apart from being particularly concerning, each point combines interesting characteristics from which lessons can be learned. Natural disasters and pandemics are old risks, in the sense that mankind has faced them constantly throughout history. Concerning them, it is essentially a question of adapting to developments, but with some differences. Climate change leads to long trends in the evolution of the risk against which one cannot easily adopt a short-term perspective, while changes of behavior may have more direct impact in a pandemic, where crisis management also plays a different role. Cyber, on the other hand, is an example of a risk that emerged so fast that its perimeter is not completely clarified, and for which a whole ecosystem of insurance solutions remains to be built.

We chose not to present these risks successively, but to identify common trends and differences, in order to provide an analysis that can be generalized to similar situations. Our paper is organized as follows. In Part I,

we begin by clarifying the concept of (non-)insurability. From the legal aspects that shapes the insurance contract, we show that the chosen definition of risk may impact its economic viability. This leads us to summarize the core elements that ensure the balance of insurance solutions, namely mutualization, and to identify how they may be endangered in the current context. The risk transfer solutions that may help to overcome these issues are taken up in Part II. We explore different types of strategies, from traditional insurance to the use of derivatives like cat bonds or parametric insurance, with a particular focus on questioning how private-public collaborations may (or may not) help in this context. Considering all the difficulties encountered by these solutions, we emphasize the necessity, for insurers, of gathering sufficient information about a risk in order to be able to properly quantify it and manage it. The question of gathering data is therefore explored in Part III. We emphasize the importance of thinking the structuration of such data in a way to be able to extract relevant information from it. In a context where shifts must be rapidly detected, or when data is rare and scarce due to the novelty of the risk, the importance of information-sharing and examples of such initiatives are stressed.

1 - Insurability

The term "insurability" can be understood at least from two angles. In section 1.1, we first explore the legal acceptance, which deals with the definition of the insurance contract itself. This legal aspect partly conditions the economic side of insurability, since it contributes to defining the perimeter of guarantees, and even to reshaping the very nature of the risk. Section 2.2 introduces the basic principles behind the economic viability of insurance contracts, including the key role of mutualization. We then explain how an imbalance can appear when it comes to emerging risks with a catastrophic component. In this case, a disaster can potentially generate an unexpected systemic event, for which diversification of risks may not be efficient if the interdependence between policyholders is not precisely known, as we describe in Section 3.3.

1.1 Legal aspect

1.1.1 Some types of coverage prohibited

The legal aspect consists in determining if a risk - or a situation related to a risk - can be covered or not through an insurance product without breaking the law. This is mainly (and logically) the approach that has been chosen by the Haut Comité Juridique de la Place financière de Paris (HCJP) in its report on the insurability of cyber risk (2022).

An interesting case concerns ransom payments. For many years, defense authorities have warned the public and private sectors against the increasing number of ransomware cyber-attacks (see the definition in Focus 1.1 below). Assuming that a cyber policyholder pays a ransom to restart its business, can insurance pay for this ransom, which is part of the losses caused by the attack? This point has created considerable tension between insurance companies and defense authorities. The French Parliament, in a 2021 report, recommended eliminating ransom payments by making them illegal (Faure-Muntian, 2021). This proposition was motivated by the fact that paying ransoms validates the economic model of hackers and thus increases the risk at a global level.

There are several difficulties that prevent banning these ransom payments, and the recent bill regarding the programming of the French Ministry of Interior has chosen to regulate this practice, without prohibiting it (see Focus 1.1 and Ministère de l'intérieur, 2022). But the important thing to notice is that regulation changes the perimeter of the risk, thus potentially modifying the extent of the claims. Ransom payments are probably harmful from the point of view of combating groups of cybercriminals. On the other hand, paying the ransom could sometimes appear to be necessary in order to unblock a very delicate situation. The example of the Colonial Pipeline attack (Eaton & Volz, 2021; Tsvetanov & Slaria, 2021) is striking: to avoid an energy shortage, the company accepted to pay a ransom of more than 2 million dollars. Although the amount was huge, the losses that would have been incurred if the company had not regained access to its data would probably have been much higher (without mentioning third party risk).

A total absence of regulation therefore has a negative global impact on the risk. But regulation that is too restrictive could make the economic equation harder to solve for insurers, since it would take away some of their freedom for resolving a crisis. Moreover, differences of regulation between countries must be taken into account: businesses wanting to be insured in case of ransom payments could turn towards foreign insurers. This competition with other insurance systems would penalize a national market by reducing its attractiveness. This is especially the case for corporate insurance, where companies can more easily turn to insurers outside the country they are based in. A non-homogeneous European response to these legal challenges could distort the competition and limit the economic efficiency of the wider market. Convergence on practices related to large risks has to be promoted in order to strengthen the stability of the protection system offered by insurance.

Focus 1.1 - Ransomware attacks and ransom payment insurance

A ransomware attack is a form of cyber-attack in which a group of cybercriminals infects servers from a company (or even of natural persons) and blocks any access to the data system. In order to unlock its system, the victim is asked to pay a ransom that may be relatively large (4 million dollars in the case of the Colonial Pipeline attack, (Eaton & Volz, 2021), see also the report of ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information, 2020), evaluating the profits of different hacker groups).

Let us mention three examples of ransomware attacks that show how critical the consequences may be:

1) Wannacry and NotPetya, two cyber-attacks in 2017 with technical similarities that each struck hundreds of thousands of computers around the world (Tourny, 2017), with losses amounting to an estimated several billion dollars in each case. This is an example of a "contagious" cyber-attack.
2) Bouygues Construction in 2019 (Mantha & García de Soto, 2021), an example of an attack against a single victim, but resulting in huge (not public) losses.
3) The Colonial Pipeline in 2021 in the US (Eaton & Volz, 2021; Tsvetanov & Slaria, 2021). Apart from the direct losses, this attack on an energy provider triggered a gas shortage in the northeastern US, and difficulties all along the supply chain.

Ransom payment insurance in cyber is to a certain extent the natural extension of guarantees that apply to the ransom of natural persons who have been abducted. Since these types of guarantees are well established in the culture of certain companies, it explains why the demand for such protection in the case of cyber is

relatively natural. The very existence of such contracts has mixed effects on the risk. In the case of kidnapping insurance, criminals may have developed a very well-thought-out system to take advantage of this type of guarantee: people benefiting from this protection are more exposed to being kidnapped, since criminals think they have better chances of getting paid. This explains why taking out this type of guarantee is (by law) confidential.

In the case of cyber risk, a major concern is the possibility of criminal groups hacking insurance companies in order to retrieve the list of businesses that have taken out a guarantee against ransom payments. Obtaining this information then leads to an increased probability of a policyholder being hacked, increasing adverse selection, and creating an imbalance that directly endangers the viability of insurance contracts.

On the other hand, regulation has failed to find the right approach to forbidding these ransom payments. There has been an effort to assimilate them with the financing of terrorism. The HCJP (2022) established that this argument could not be used, since cybercriminal groups cannot be directly assimilated to terrorist groups. The only exception would be if the victim had direct knowledge making it possible to affirm that the attacker was a terrorist group.

After a report of the French Parliament in 2021 recommending clarifying the question of ransom payments through prohibition, a governmental proposal took another direction (Ministère de l'intérieur, 2022, article 4), promoting regulation: the victim should first report the attack to the police before thinking of paying the ransom. This measure was also introduced to avoid the development of invisible payment systems.

1.1.2 Exclusion clauses in the policies

Although legal clauses may make it possible to redefine what is covered and what is excluded, this can also be imposed by the market itself to protect against claims that are too large. An emblematic example, in the case of pandemic, is related to the exclusion of business closures caused by administrative intervention. Such a clause is inserted in order to avoid a global phenomenon endangering the ability of the portfolio to absorb the risk, since every policy would be affected at the same time.

In the case of cyber risk, a good example is the exclusion of "State-sponsored attacks" promoted by Lloyd's (Lloyd's London, 2022). The principle is the following: war is a classical exclusion clause in insurance policies. Since States seem to be behind many of the cyber incidents (Ferland, 2019; Agence Nationale de la Sécurité des Systèmes d'Information, 2020), these acts may be assimilated with war. This argument was previously used in the Mondelez case, related to the NotPetya attack (Ferland, 2019), but it is interesting to note that the term "war" is replaced, in the Lloyd's case, by the concept of "State-sponsored" attack since no formal declaration of (only) cyber war existed in the past. Nevertheless, the robustness of such clauses, or even their feasibility given local legislation, may still be questionable: the exact definition of a State-sponsored action is not completely clear, especially in a context where many groups of cyber criminals seem to operate with the blessing of States, and may be composed of former or active employees of a State. Potential disputes on the legal qualification of some events may add uncertainties to the outcome of a claim. The recent report of the French Treasury Department (Direction Générale du Trésor, 2022) pointed out the necessity of clarifying this concept of cyber war.

Examples of such disputes around the qualification of claims can also be caused by lack of anticipation of the consequences of an event. The case of restaurant closures in France is enlightening: some insurers invoked a clause related to the administrative closure decided by local authorities to justify refusing any compensation for policyholders (Poullennec, 2021). The resulting tension between both sides was related to the fact that this clause was not necessarily understood by the public as applicable to such an event. Without judging the legitimacy of such an action, let us note that it would be preferable if exclusion clauses were as clear as possible for all parties involved (not only on the legal side, but also for how these clauses are perceived by the public). Indeed, these tensions can create a negative perception of the insurance market, and potentially discourage policyholders from relying on such coverage solutions.

1.1.3 Conclusion on legal aspects of insurability

Although we will mostly focus on insurability viewed as economic sustainability of a risk, the legal framework plays an important role since it can, by itself, modify the very structure of the risk. Extending the period for declaring a claim (for example in the case of drought) increases the probability of a claim being made, at least from the insurer's perspective (some claims that were made would not have been reported otherwise, and so would have been considered as inexistent within the scope of the insurance contract). This thus mechanically increases the economic cost, showing there is a link with the technical side of insurability that we address below.

Legal exclusion of some components of a risk aims at protecting the customer or, more generally, the public. In the case of ransom payments, regulation is necessary to avoid supporting cyber criminals who would see their economic model validated. Exclusions that are not mandatory but included by the insurer in the policies also serve the general interest, in the sense that they are designed to avoid endangering the solvency of the insurer because of the catastrophic or systemic event that we describe below. However, we should point out that the lack of homogeneity between European countries regarding the legal framework (as in the case of cyber ransom payments) can create distortions that may be counterproductive.

Nevertheless, the legal perspective cannot entirely address the question of insurability, which is not the only issue in designing a contract. A limited use of exclusions (by law or through initiatives of the insurer) should be recommended. As we have already mentioned, redefining the perimeter of coverage is one way to reframe the risk, but it does not make the risk disappear. In the end, insurance cannot avoid facing the challenges raised by risk without losing its purpose, hence its attractiveness for policyholders. We will see in the following section that this attractiveness is also a key element, since it helps to reach a volume of policies essential for ensuring solvency.

1.2 Economic aspect

The core of an insurance system is the mutualization principle. By bearing the risk of a large number of policyholders, the insurer reduces the uncertainty related to the outcome of a given period: the insurer will probably suffer from losses but be compensated by the fact that many policyholders make no claims, while they still pay premiums. The robustness of this system is based on mathematical calculations, which should nevertheless not be considered as guaranteeing the automaticity of this mutualization process. Balancing the

payments of policyholders with claim payouts by the insurer requires effort: as for every mathematical result, the mutualization equation is based on assumptions, which can be easily challenged if the model seems endangered.

Focus - 1.2 Mutualization

Technical mutualization is the consequence of results coming from risk theory (Grandell, 2012). Risk theory is used to deal with uncertain outcomes, and the first thing to understand is that an element of randomness should be present if one expects to take advantage of these results: if the outcome of a risk is known in advance, the problem results in simply dividing up the loss between stakeholders. Here, the idea is to consider that, at a macroscopic level (that is, when one puts together many policyholders), the outcome is almost certain (hence the losses can be split between the members of the community through the premium they pay), while it can remain very uncertain at an individual level (for example, coming losses of policyholders may be inexistent in most cases, but each policyholder has a significant probability of making some claim, whose amount may also be very uncertain).

Of course, uncertainty is not erased by the mathematical results behind mutualization. Different levers or conditions determine whether a portfolio's situation resembles or not this idealized behavior. Below we list the main technical conditions, while explaining how they translate concretely into a business perspective.

- Independence between policyholders: if one knows that a claim affects a policyholder, it should not affect the probability of another policyholder being affected. This is a common assumption in car insurance: if the portfolio is large, the probability of two specific policyholders colliding with each other should be very small. On the other hand, in natural disasters, this assumption may not hold: policyholders living near the same forest will be simultaneously affected if a fire occurs. Diversification strategies exist to accommodate for this dependence between policies and reduce its impact on mutualization.

- Similarity between policyholders: if policyholders are not exposed in the same way to the risk, or behave differently, this may add some volatility to the outcome. Mutualization does not break down, but the difference between the outcome and what was predicted can become larger. Understanding the impact of the characteristics of the policyholders is therefore key to reducing this volatility.

- "Finiteness of the risk": this technical assumption is related to the concept of mathematical expectation. To understand basically what it means, some risks are so volatile that the traditional notion of volatility (linked to mathematical variance) is not adaptable, making such classical tools as modern portfolio theory irrelevant. For such cases, restrictive limits to policies should be established since one is flirting with the frontier of technical insurability.

- Large number of policyholders: the size of the portfolio is key to achieving proper absorption of risk.

- Statistical estimation: in practice, a statistical analysis of prior experience with the risk is required to build a proper mutualization framework. But this statistical analysis may be of poor quality, if based on irrelevant or scarce data. This adds some volatility and reduces the ability to carry out proper mutualization.

1.2.1 Attractiveness of the contract

Let us focus on two points that seem essential, and that go beyond the mathematics of actuarial evaluation:
- the premium paid by the policyholder should be small;
- the number of policyholders in the portfolio should be as large as possible.

These two points are linked: if the premium is too large, the number of policyholders will decrease, except in the case of mandatory insurance. In all cases, large premiums are a burden that will lower the profitability of companies that are insured and impact natural persons' income. On the other hand, the premium paid by the policyholder does not only reflect the most likely situations but is also there to build up sufficiently large reserves to absorb pessimistic scenarios whose probability of occurrence is high enough to be a matter of concern.

The Conseil Économique, Social et Environnemental (CESE, Economic, Social, and Environmental Council) (2022) describes the case of agricultural insurance, for which the coverage rate of the sector is particularly low, pointing to the low incomes of some people in the sector. In this context, prices are seen as prohibitive, even though the sector is particularly exposed to the effects of climate change.

The recent Lucy report from AMRAE (Association pour le Management des Risques et des Assurances de l'Entreprise [Association for Corporate Risk and Insurance Management], 2022) on cyber insurance identifies the increase in premium costs and the declining insurance capacity as factors that explain a decrease in the number of large companies that take out cyber insurance. The report calculates the increase of the typical premium amount to be around 43% between 2020 and 2021 for large groups, while capacities decreased 23%. Deductibles also increased (although the report does not give clear comparisons with previous numbers).

This development follows a 2020 fiscal year that was very poor, with an estimated loss ratio of 167% for the market. So it was logical to make a correction in an attempt to reach a balance, in a context where risk seemed to be inadequately priced. We see that all the various levers were used (deductibles, capacities, increased premiums) to try to achieve economic balance. But this deterioration in the policy content can have consequences. According to AMRAE, among large companies, around 4% consequently chose not to take out cyber insurance anymore and to assume this risk on their own. This analysis should be tempered by the fact that, at the same time, mid-size companies took out 20% of cyber insurance contracts, according to the report. But these smaller businesses may not have the same ability to turn towards other solutions, given the current situation.

Although we should not overinterpret the conclusions of this report, it is important to note that the lack of attractiveness of some insurance contracts (which, in the end, do not respond to the demand that led to their introduction) is a real concern, since the volume effect is key in the economic viability of insurance contracts.

If one looks at the comparison of the LUCY numbers with the loss ratios of cyber insurers published for the US market (National Association of Insurance Commissioners, 2020), one sees dissimilarities between players. Although the method of how these ratios were computed is unclear (the methodology is not necessarily homogeneous, and probably not perfectly comparable with AMRAE numbers obtained from brokers), the insurers with the highest market share tend to enjoy better results (61% loss ratio for the leader, Chubb, which had 14% of market share). This tends to confirm that volume is a way to absorb significative claims.

Moreover, a small portfolio can lead to a higher safety premium in order to achieve the prudential requirements of the insurer (AMRAE, 2022).

1.2.2 Systemic risk

A rigorous definition of systemic risk first requires defining a system that is susceptible to fail. For example, the term is used to define the potential simultaneous failure of different financial institutions in credit risk (Schwarcz, 2008). Let us first point out that we use here a more general and improper vision of systemic risk, in the sense that the scale of failure may not necessarily be understood as a failure of the global insurance system but may be limited to the perimeter of a single portfolio.

A portfolio can fail essentially because of an increase in the severity or the frequency of claims. In some particular cases, a single policy can lead to a particularly high loss that may endanger the solvency of the insurer. A classical historical example is the case of the car accident of March 18, 1976, in France, which led to a train accident, whose cost for the insurer is now estimated at 3 billion francs (approximately 19 million euros). Nevertheless, for emerging risks, policy limits are a common way to ensure protection against such high claims. So, in our context, the concept of severity has to be understood as the scale of an event, one that simultaneously strikes a large number of policyholders, like the Katrina hurricane or the Lothar and Martin storms.

In this case, the damages do not need to be huge: the cumulated damages caused by a single systemic event can be high, while every policyholder may experience a moderate loss. For example, pandemic scenarios defined during the H1N1 crisis expressed worries about such kind of situations. Lloyds (2018) listed the different guarantees that might be impacted by a pandemic as estimated in 2005. The report seemed to miss, at that time, the impact of business closures: this point was discussed, but as a "secondary impact", considering that history did not plead for the plausibility of such a threat. However, the different scenarios that were considered showed a possible accumulation of relatively small claims leading to a strong impact. In this configuration, the size of the portfolio plays against the insurer, since everyone is hit at the same time, showing that the mutualization principle does not apply here.

Such crises episodes may still be absorbed if they are rare. They are not expected, and the formerly collected premiums were not necessarily meant to cover such an event, but a single peak might be absorbed. This requires, of course, a situation where the reserves are sufficiently high. But a company can survive a year of

negative results if profitability is rapidly restored. The question is the possible repetition of such episodes, which, after considering the question of severity, brings us to the even more challenging case of frequency.

To take the example of climate risk, the current projections of climatologists (Zhongming et al., 2022) indicate that the increase of global temperature should significantly increase the number of catastrophic episodes like Lothar and Martin in Europe, or the drought of 2003. The extreme episodes experienced in Europe in the summers of 2021 – important flooding in Germany (Fekete & Sandholz, 2021) and the Alex storm in France (Bafoil, 2022) and 2022 drought and fires (Copernicus, 2022) – are warning signs that corroborate this trend. As long as extreme events remain rare, their impact is relatively low, since it is mitigated by the small probability of occurrence. But if their frequency starts running too high, they cannot be considered as "peaks", but as a new normal leading to a significant increase in premiums.

Focus 1.3 - Examples of systemic risk scenarios

Defining systemic risk scenarios is important for testing the resilience of insurance portfolios and organizations. It is not necessarily a matter of pricing, but a way of anticipating the total reserves required, to identify prevention measures, and to anticipate crisis management policies. Examples:

- Natural disasters: one may distinguish scenarios that are based on local specificities from scenarios at a national or continental level. The Caisse Centrale de Réassurance (2016) established scenarios of a huge flood of the Seine, taking into account the impact on an area characterized by high population density and a concentration of economic activity. The Institut des Hautes Études pour la Défense Nationale (2020) imagined a scenario comprising the conjunction of high temperatures in a context of persistent rainfall deficit. Agriculture is severely affected, hospitals are overwhelmed, nuclear power plants are forced to shut down, and riots occur. This scenario of destabilization of a whole country goes far beyond the simple field of insurance but shows the possibility of a climate event contaminating other risks, with potential consequences for various types of guarantees.

- Pandemic: the consequences of Covid-19 may now be analyzed to reevaluate pandemic scenarios. But it is interesting to compare this with the scenarios imagined beforehand. Lloyds (2018) summarizes the potential consequences, viewed from the period of the H1N1 crisis. We have already mentioned the difficulty of properly evaluating the precise circumstances of the next catastrophe (with, in the case of the pandemic, the underestimation of the consequences linked to business closures). This difficulty is linked to the fact that epidemics do not follow the same path depending on the type of viruses (level of contagiousness, categories of population more exposed…). For example, the H1N1 crisis focused attention on a virus like the flu spreading, with a high mortality rate among the young generation. Covid-19 turned out to be different.

- Cyber risk: Institut Montaigne (2019) describes a so-called "cyber hurricane", evaluating the potential consequences resulting from an attack that hits the entire society. More precise scenarios are related to measuring the consequences of an attack on a cloud provider, for example. Asensio et al. (2022) evaluate the consequences of such an attack on financial activities. Behind these studies, one sees the specific difficulty related to cyber: many users may share the same software or digital product, making them

simultaneously vulnerable if this service is targeted (or interrupted, even for no malicious reason). However, the wealth of solutions, and the difficulty of apprehending this new technological risk makes it difficult to anticipate all cases, and even to precisely identify all weaknesses.

1.3 Diversification

Diversification is a classical way to protect a portfolio (both in finance and insurance) against the systematic failure of its components. In finance, modern portfolio theory makes it possible to define optimal investment strategies based on correlations between assets. A well-balanced proportion of anti-correlated assets ensures that a depreciation of some of them will be compensated by the performance of others. A classic example of anti-correlation is assets related to airline companies and oil prices: a high oil price usually has a negative impact on the performance of airlines.

In insurance, putting together a portfolio based on a similar diversification principle faces several difficulties:

- the availability of the "assets" (that is, the policyholders): the insurance company can less freely impose a given proportion of some class of risk, since acquiring new customers is harder. Nevertheless, strategies to underwrite policies for more customers of a given type are possible.
- the correlations are less obvious. In finance, considerable data on prices is available in order to establish a relatively clear view of the correlations (although correlations can change over time).

Nevertheless, financial markets may have their role to play in using anti correlation for risk protection. For example, this is a key idea behind the attractiveness of cat bonds, which are described more extensively below. However, the intensity of some catastrophic events may have impacts beyond the usual perimeter of the risk: Covid-19 is a good example of a pandemic crisis with effects on various sectors of the economy that may have seemed uncorrelated with the health sector.

However, in finance it is well known that correlation analysis is no guarantee for protecting a portfolio during a crisis. When the entire market falls, negative correlation is not enough to protect investments. Similar things happen with insured risk. A good example is the case of natural disasters. In this context, diversification consists, for example, in avoiding too large a proportion of the portfolio living near the same river (in the case of flood insurance). Although it may be difficult to define optimal rules to ensure this geographical diversification, guidelines already exist that define underwriting rules in order to avoid this issue. In this case, diversification is not a direct means to optimize the volatility of the result, but a basic measure of protection to avoid systemic risk.

But this essential measure may be difficult to apply to risks where relations between users are not clear. Cyber risk is particularly telling in this context. The geographic proximity is not completely absent - the NotPetya attack struck Ukraine first and primarily infected companies with links to Ukraine. But it is difficult to determine the proximity between players in a dematerialized world of exchanges. Particular attention should be devoted to a better understanding of these connections. Right now, insurance companies have too little information about the tech environment of their policyholders, which strongly limits the ability to carry out this analysis.

The Solar Wind attack in 2019 (Martínez & Durán, 2021) was, however, a warning sign. After breaching a single software program, which was widely used by the US administration and industries, hackers managed to simultaneously infect a large number of victims. Since this attack was motivated by espionage (probably from a State), the damages did not generate large losses, unlike an attack whose aim is destruction or financial profit, but the danger was obvious: by infiltrating a single software provider, all its users can potentially be hit at the same time. But identifying such systemic vulnerability would require, from the insurers' side, better understanding the technological environment of their policyholders. With their collective vision at a portfolio level, insurers benefit from a privileged position to undertake this analysis and potentially detect vulnerabilities, which could also be useful for improving national security.

1.4 Analysis of insurability challenges

Under the new paradigm imposed by large emerging risks, the most obvious means to achieve insurability are:

- limiting potential losses through the introduction of exclusions in policies or by law;
- increasing the price of premiums in order to deal with increasing frequency and severity.

Excluding and increasing the premium cannot be the only responses. Limiting the perimeter of policies discourages potential policyholders from relying on insurance, thus reducing the volume of insured, which is necessary to succeed in mutualizing risk. Increasing the cost of the premium leads to abandoning one of the fundamental principles that we mentioned earlier: the insurance premium should remain affordable. In the end, using only these two levers leads to a situation where insurance more or less gives up covering the risk.

Meeting this challenge requires actively exploring elaborate solutions that can avoid the insurer having to simply bear the risk. In the next section, we explore the possibilities offered by risk transfer, from classical reinsurance to innovative techniques. The combination of such possibilities offers various degrees of freedom to improve economic viability. Nevertheless, the observations we have made in this section already suggest that efficient deployment of such strategies requires a better understanding of the risk itself. We mentioned previously, in section 1.3, that insurance companies benefit from a precious advantage with their ability to collect information. The use of such wealth will be discussed in Part III.

2 - Risk transfer

Risk transfer solutions make it possible to shift some part of the risk to another party and are essential for the economic viability of an insurance system when potential losses may be large. Let us note that introducing limits to policies or excluding some situations is probably the most basic risk transfer method, since the uncovered part of the risk is directly transferred to the policyholder. The purpose of more technical solutions is precisely to avoid downgrading the coverage from the policyholder's point of view; it involves instead transferring excessive risk to another party.

Another possible advantage of risk transfer solutions (like parametric insurance or catbonds) is also to simplify claim management. The idea is not to insure directly against the risk, but to rely on an indicator or a derivative

that is simpler to control and measure and is still correlated with the concerns of the policyholder. As a consequence, one may fluidify the compensation procedure for the policyholder, which sometimes can finally reduce the long-term costs by providing efficient and quick reparation.

In this part, we explore these different solutions. Starting with classical reinsurance in section 2.1, and the potential for collaboration between the public and private sphere in section 2.2, we then describe how capital markets can play a role in absorbing part of the risk through Insurance Linked Securities in section 2.3. Tools like parametric insurance, which can also be vectors of introduction of securitization, are described in section 2.4. Section 2.5 is then devoted to the need to reinforce prevention. Investing in prevention can be seen as a form of risk transfer, since efforts are made to fight against the changing risk. Facing the emergence or the changing risk and weighing on the behavior of policyholders is indeed crucial in going beyond the acknowledgement of a growing threat.

2.1 Reinsurance

2.1.1 Reinsurance faced with an increase in severity and frequency

Reinsurance is risk transfer to another insurance company. The two most classical situations are proportional reinsurance and stop-loss agreements. In the proportional case, the insurer receives compensation from the reinsurer for a proportion of the total losses of the insurer's portfolio. The stop-loss contract defines a threshold: if a claim (or the global amount of claims depending on the contract) exceeds some level that can be understood as a deductible, the reinsurance company must compensate the insurer.

The economic validity of this type of solution depends on the insurance companies transferring part of the risk but remaining the unique partner of the policyholder. Consequently, the claim management expenses, and the costs related to the collection of the premium are not transferred to the reinsurer, which makes it possible to be profitable.

Stop-loss treaties are very appealing for the policyholder in the context of a risk with potentially catastrophic claims. This is a way to lower the limit of the insurance policy without redrawing it (which would reduce its attractiveness and could discourage potential customers). Compared to a proportional agreement, this type of contract also possesses the advantage of implicitly (partially) protecting the insurer against "model risk" - the premium price is indeed a function of the various projections based on models and commercial constraints. If the projections are wrong, the losses may be much higher than expected. If this occurs, the stop-loss contract helps the insurer limit the burden of this underestimated risk.

Nevertheless, this additional burden does not disappear and affects the reinsurer. Hence reinsurance should not be understood as a way to absorb all uncertainties related to the anticipation of risk. Moreover, this absorption is only possible if such extreme losses are not frequently repeated. Reinsurance may be efficient in dealing with an increase in severity, but only if severity stays contained, that is, remains infrequent.

Regarding emerging risks, reinsurance is invaluable, since it offers protection against the manifold uncertainties related to the anticipation of losses. However, Pastré & Albouy (2021) point to the difficulty for reinsurers to offer affordable premiums in this context (Pastré & Albouy, 2021, p.27): uncertainty also applies

to them and tends to increase prices that then concern the whole market. Among the challenges faced by modern reinsurance, Pastré & Albouy (2021) stress the important need for reinsurer capital, noting the concern that the traditional assets used to constitute it - traditionally real estate - may be affected by the same events that cause huge losses -, natural disasters, for example. Their role of diversification, essential in reinsurance to counterbalance the cyclicality of the activity, no longer functions.

Among the recommendations proposed by Pastré & Albouy (2021) is a convergence between insurers and reinsurers in order to improve efficiency. The authors also plead for a long-term vision of capital - denouncing the rule of prudential directives that require a short-term vision of the results and solvency of companies - similar to the mutualist system: the mutualist approach indeed has the ability to create capital by accumulating annual positive results. In view of the observations, we made in section 2.B., this long-term vision is appealing - it makes it possible to absorb the "peak" effect of a particularly severe exercise.

2.1.2 Reinsurance captives

A captive, strictly speaking, is no risk transfer tool since the risk it covers remains inside the company to which the captive belongs. Let us, however, address this point as an additional means of financing risk besides the other mechanisms reviewed above.

Reinsurance captive is indeed also one way for a company to finance part of the emerging risks. It is an internal vehicle set up at a company level to finance its own risks and mutualize risks amongst its affiliates over time. This solution is therefore essentially the prerogative of large companies. Captives may initially be a response to the difficulty of finding proper coverage due to the lack of appetite of the insurance markets for extremely high risks. In addition to this function of filling the gaps between the available offers, captive may result in a virtuous circle in the behavior of the company that uses this device.

For a captive, there is no separation, unlike traditional insurance, between the policyholder that makes the claim and the insurance company that is subjected to financially repairing the risk. Here, risk and its consequence stay within the same company, encouraging it to promote a culture of risk, develop internal loss prevention policies, and improve the quality of the risk. These elements are not specific to companies relying on captives - although moral hazard is often mentioned as potentially endangering the balance of insurance systems, large risks have consequences so great for a victim that it may not seem relevant to assess whether taking out insurance would be a way to avoid implementing prevention strategies (see section 2.5 later). However, resorting to a captive creates an additional incentive to enhance prevention, while its very existence requires a deep, rigorous analysis that is the concrete expression of the company's efforts to identify risks and eliminate them. Hence, the fact that a company has developed its own captive should be seen as a positive risk factor when buying traditional insurance products.

The development of such captives has not been consistent in Europe due to differences of regulation. Countries like Luxembourg, Malta or Ireland have established rules that allow the captive to free itself from some of the constraints that apply to the traditional insurance industry. Behind this favorable regime, the idea is to acknowledge the specific difficulties of these vehicles, whose goal is to insure extreme risks that the market itself is often reluctant to take on.

The report of the French Treasury Department (Direction Générale du Trésor, 2022) outlines the positive effect of the development of captives for the spread of cyber insurance in an efficient sharing of the risk among insurers and policyholders. It favors thinking about how to make the current regulation shift in the direction of more flexibly mixing self-insurance and transfers to the insurance market.

2.2 Public / Private solution

As pointed out by the Conseil Économique, Social et Environnemental (2022), when a risk becomes a too heavy a burden, private insurance solutions cannot cover all the losses due to their limited capacity and a failure of the mutualization principle. State intervention can then appear as a solution to help the sector. The French "Catastrophes naturelles" (CatNat) regime is an example of collaboration between public and private stakeholders. This regime, established in 1982, is a public/private partnership. Paying for this guarantee is mandatory when one takes out an insurance contract that offers protection against property damages. A percentage (fixed by the law) of the premium paid for property damage contracts is devoted to the CatNat regime. The perimeter and rules of the guarantee (time limits for making a claim, deductibles…) are strictly defined by law. Natural disasters covered by this guarantee are typically floods, mudslides, landslides, earthquakes, and drought. Let us note that storms, hail, and excessive snow episodes are not included, although it is also required that specific coverage for storms be included in every policy.

The guarantees are triggered through a particular procedure, which depends on the publication of a governmental decree stating that a given zone, at a given time, is eligible. This decree is drafted by an inter-ministerial commission, which takes up requests from mayors who want a given event to be recognized as exceptional. The process generally takes about 18 months.

The fact that the guarantee is mandatory is a way of increasing the number of premiums dedicated to this risk and of reinforcing mutualization. Insurers also benefit from unlimited reinsurance coverage since State ultimately guarantees sufficient capacity to deal with the potential catastrophe.

The CATEX plan proposed by France Assureurs in 2020 (Conseil Économique, Social et Environnemental, 2022, p.38 and France Assureurs, 2020) was an attempt to strengthen protection (against administrative closures linked to pandemics) based on a mandatory contribution. The plan, which was finally rejected, was based on public/private interaction, and the fact that a sufficient number of premiums would have been collected, since all businesses would have been forced to contribute. This mandatory insurance was not necessarily popular - which is one of the reasons behind the rejection of the proposition - because it increased the cost of insurance premiums for businesses. The increased premium cost was seen as impacting business competitiveness. Companies that were not convinced of the reality (or severity) of the risk were reluctant to pay higher prices.

In the Faure-Muntian (2021) report on cyber insurance, another type of strategy was proposed to get around this reluctance, while still increasing the sum of premiums allocated to a major risk. To deal with the lack of businesses subscribing cyber insurance contracts, it was proposed that this type of guarantee be mandatory for companies doing business with the public sector.

In any case, the question of harmonizing and articulating these types of responses at a European level seems key for at least two reasons: first of all, the European level seems to be the right dimension for responding to risks that can lead to such large losses and that are not contained by physical borders. The huge financial capability that is required to meet catastrophes related to these new risks can be more efficiently created through cooperation between States. Second, the disparity between national responses can distort the competition between companies. The key role of such mechanisms in absorbing the shocks would mechanically weaken companies that do not benefit from efficient State collaboration. However, designing such a European mechanism would require starting from scratch. The culture of risk and insurance protection is different from one country to another, and an attempt to generalize a particular protection system to all European countries would probably not be successful. While lessons must be learnt from models that seem to work well (like the CatNat regime in France), applying them to other kinds of frameworks and environments does not guarantee an efficient system. Moreover, the key difficulty is to elaborate a system at a European level that could unify approaches without disrupting mechanisms that are currently working well at the national level.

2.3 Insurance Linked Securities

Insurance Linked Securities are financial products allowing insurers to transfer risk to financial markets. Catbonds and weather derivatives are a good example. The coupons and principal payments of catbonds depend on an index of natural disasters. In the absence of a catastrophe, the payout of a catbond is like a classical bond. But if the disaster does occur, the principal is used to pay for the losses.

For investors, the nice feature of catbonds is their low correlation with other traditional securities. They can be used to enhance portfolio diversification. The second appealing characteristic is the rate of return they propose. These rates include a "risk premium" linked to the potential loss of principal if the disaster occurs.

Beyond these two features, the model is based on two main assumptions:

- the absence of a link between natural disasters and non-related financial products, which is a form of diversification. This assumption may not hold if disasters affect a significant part of the economy. For example, an energy shortage triggered by a natural disaster could have important industrial consequences that may impact financial markets.
- the frequency of catastrophes must be sufficiently low. If the frequency increases considerably, the rate of returns can be adjusted to compensate, but only to a limited extent.

So, these tools are strong enough to absorb the transfer of a "severity" risk, but not of a "frequency" risk. Moreover, to be sufficiently attractive for investors, the absence of correlation feature may limit their use for certain risks. Cyber is a good counterexample: a significant part of cyber risk is human-driven. Hackers can adapt their strategy to the current weakness of their target. A recent example was the opportunistic use of the Covid-19 crisis by cybercriminals – increasing the pressure on the health sector to make ransom payments (Lallie et al. 2021). These groups may thus have the possibility of creating or increasing correlations with other risks that could disrupt the market. In addition, Pastré & Albouy (2021) question the future growth of such

forms of risk transfer, if they only allow, by design, transferring a small part of the risk (less than 10% of insured amounts).

Focus 2.1: Catbonds and pandemic bonds

According to the 2021 ILS Annual Report from Aon (Bloomberg, 2020), the market for catbonds experienced strong growth between 2020 and 2021. Approximately $13 billion was invested in the period between July 2020 and June 2021, compared with $9 billion in the prior year. The types of catastrophes covered are essentially natural disasters: earthquakes, typhoons, named storms in designated areas. Products related to life and health insurance also exist.

With the Covid-19 crisis, the idea of developing "pandemic bonds" has gained ground. The idea of pandemic bonds existed prior to the crisis: this solution was promoted by the World Bank President Jim Yong Kim in 2015 after an Ebola outbreak, for example (Bloomberg, 2020). For a pandemic bond, the catastrophe triggering the guarantee is when an epidemic produces a certain number of victims. Concerns about the viability of these bonds are twofold:

- it is difficult to properly evaluate the probability of occurrence (this is always the case for catbonds, but the example of Covid-19 shows that the pandemic risk was under evaluated compared to the models used during the H1N1 crisis)
- the non-correlation with traditional financial products does not seem certain, since the Covid-19 crisis generated a global depreciation of markets.

An attempt to promote a system of pandemic bonds was developed by the World Bank in 2017. The complexity of the triggering condition played a role in the failure of this instrument to respond to the need: technical conditions were introduced that were not necessarily easy to certify, with differences between the type of viruses (Ebola, flu…) causing the pandemic. The 2018 Ebola epidemic in Congo did not trigger the bonds, although they were initially designed to activate in such situations.

2.4 Parametric insurance

Parametric insurance consists in not directly insuring the risk itself, but a parameter (meaning an index) which is thought to be correlated to it. This parameter can be viewed as a simplified representation of the risk itself. For example, a weather index can be used to define the intensity of a drought episode, like the Standardized Soil Wetness Index (SSWI) (Soubeyroux et al., 2012), or of an intensive rain episode, like the Standardized Precipitation Index (SPI) (Vidal & Wade S. (2009). The compensation received by the insured party can be computed on the sole basis of this parameter, without looking at the real effective losses.

The appealing features of parametric insurance are twofold:

- it considerably simplifies claim management. Since the parameter is supposed to be easily available shortly after the event, the amount of the claim can be determined very quickly. Compensation can be rapidly sent to the victim without the necessity of additional expertise. For the policyholder, the quick payout of

compensation is appealing - the victim can quickly use this amount to begin repairs after having made the claim;

- the task of the insurer in creating its economic model is simplified, since modeling the evolution of this parameter is usually simpler than modeling the consequences of the risk itself. Hence, solvency requirements are easier to compute and control.

Parametric insurance is frequently promoted as a solution for responding to the losses generated by climate change (Broberg, 2020; Horton, 2018), especially through its ability to quickly compensate deprived and/or isolated territories. Johnson (2021), however, has noted the consequences of potential disappointments of policyholders with parametric insurance. Johnson (2021) gives the example of agricultural insurance in Africa, where "ex-gratia" mechanisms had to be established to appease the public when the parametric approach failed to respond to the needs of the victims. It is important to understand that this component will always exist, even for well-designed parametric products, since this is a structural characteristic of these solutions: relying on a parameter consists of simplifying the problem. Simplification has a cost: one cannot expect the parameter to correspond exactly to the basic risk itself, especially when the basic risk is highly volatile (one of the purposes of introducing a parameter is to reduce volatility).

Thus, in our opinion, parametric solutions are promising but are not miracle solutions that alone can ensure coverage of the risk. They should be considered as tools that should necessarily be combined with more traditional insurance or risk transfer strategies. They present the key advantage of making it possible to quickly compensate the policyholder. This feature is particularly useful in a context where the frequency of claims tends to increase: if compensation is delayed, reparations are delayed, and future claims may have even more dramatic consequences. By introducing a parameter, they also make it possible to potentially create derivatives based on this parameter, which is another way to improve risk transfer. But careful attention should be devoted to the selection of an appropriate parameter (whose connection to the risk should be scientifically established and controlled over time), and to harmonizing the role of parametric products as part of a diversified pool of coverage instruments.

Focus 2.2: Parametric Insurance solutions.

Here are some examples of parameters (or indexes) used to cover different kinds of risks. In a parametric product, the amount of compensation is solely determined by the value of the parameter. Parameters of course can be adapted to the exposition in the area concerned by the coverage.

Parameter	*Risk covered*
Magnitude of an earthquake	Seismic risk
Category of a hurricane	Natural disaster
Precipitation levels	Flood
Time of business interruption	Cyber risk
Number of records (i.e. amount of data) leaked	Cyber risk

In each case, the parameter is obviously correlated to the risk being covered. But is this correlation strong enough? While the relationship between the parameter and the severity is obvious for physically well understood phenomena like natural disasters, this may not be the case with cyber, for example. An interruption of a few hours of an online service may have different consequences depending on the period when the victim was affected and on the sector of activity. In this case, the parameter should be properly tailored to take different situations into account.

However, parametric insurance has important limits:

- insuring a parameter is not the same as directly paying for the risk: sometimes, the compensation of a parametric insurance contract can be deceptive. The parameter is supposed to be correlated with the real loss, but this correlation is not perfect, especially for very large claims.
- selling parametric insurance is complex: one must convince the policyholder that the parameter correctly reflects the risk against which he/she is looking for protection. This is particularly the case for risks that are difficult to appreciate, like cyber. While a meteorological index will clearly be seen as related to natural disasters, the physical reality of indexes related to cyber can be less convincing for the customer. Moreover, the parameter needs to be readily available - the policyholder needs this so as to ensure transparency and the parameter must also remain available over time for the insurance company in order to maintain the guarantee.
- choosing the proper parameter is a challenging task. A relatively large amount of preliminary data is required to check if the parameter is properly correlated to the risk and is the proper metric to be used in insurance.

Focus 2.3: Parametric insurance and large claims

Parametric insurance products have been created so that, on average, they make it possible to properly cover the risk. The term "on average", which comes from risk theory used for the calibration of such instruments, obscures the fact that, for two distinct claims, the situation may be quite different from the policyholder's point of view. "Remainder" is the term often used to qualify the difference between the losses generated by the basic risk and the compensation received by the policyholder. For typical claims (that is, claims corresponding to the average scenario), the Remainder may be positive or negative, but tends to be small compared to the real loss. This means that the policyholder is either overcompensated or disappointed, but the disappointment is relatively low since most of the loss has been covered. Moreover, the rapidity of the compensation process can help lessen this disappointment. However, if a claim has particularly strong consequences, the Remainder tends to be systematically smaller than the true loss, as shown in Lopez & Thomas (2022). This structural feature is the consequence of lower volatility of the parameter compared to the basic risk. The result of lower volatility is that there is a lack of planning for "exceptional" claims, leading to poor coverage in these situations. The term "exceptional" should not be mistaken: although the probability of such claims occurring is structurally low, these situations are not purely fictional, and actually occur with sufficient frequency to be of concern. The consequences of such a mismatch may also lead to such contracts being less attractive - the failure of parametric insurance to properly cover highly publicized catastrophes can lead to its more frequent successes being overlooked.

2.5 Prevention

Prevention can be understood, to some extent, as the transfer of a part of a risk through the investment made (by the policyholder, the insurance company, or public authorities…) in order to avoid claims being made. The role of prevention is key in a context where a risk changes and/or when it seems to reach levels that directly question insurability: by reducing the burden caused by the cost of claims, it may be possible to slow down negative trends.

In the case of climate change, the question of learning how to live in a world with frequent extreme meteorological phenomena is often raised (Smilyanets, 2021). Prevention can be seen as a way to acknowledge change, and to promote the necessity of modifying behaviors so that the consequences of extreme weather may be less critical. Rethinking the way homes are built, questioning the location of houses in a given area, and building protections against flooding are examples of ways to invest in prevention. For cyber risk, prevention is also at the core of the insurance procedure, first with questionnaires that help the policyholder identify potential weaknesses, but also through the positioning of some third-party actors who endeavor to provide guidelines to policyholders (and information to the insurance companies) so that they "become insurable" after implementing the appropriate procedures.

On the other hand, particular attention should be devoted to insurance coverage not being seen as a way to eliminate the need for prevention. The case of public / private collaboration could be of concern in this perspective. With the illusion of absolute protection - since public intervention may be seen by the public as having no limit - the absence of changes in behavior is to be feared. Although it is hard to precisely quantify such an effect, this type of negative behavior is mentioned in Latruffe & Picard (2005), for example, whose analysis takes up many similar historical natural disasters (Barry, 2020). In the absence of changes in behavior, the growing risk would not be contained, and any insurance solution could become non-viable in the long (or even medium) term. Therefore, it seems crucial to strongly promote incentives for positive behavior by the policyholder.

Another difficulty is the potential lack of knowledge about the effectiveness of prevention measures. The example of the business closures caused by the Covid-19 pandemic is particularly striking (Chowdhury et al., 2021). Securing the supply chain is one of the key objectives of risk management for companies, and the activation of some continuity plans should have theoretically been planned years before the crisis. But the difficulty of anticipating the exact consequences of the catastrophe made some alternate ways of supply unexpectedly unsure, creating difficulties for some industries. In this case, many theoretically resilient organizations appeared to be much more fragile than expected. This shows the importance of scenario building. But to properly anticipate the catastrophe, it is necessary to properly understand the risk, to understand if a given solution is effective in reducing the frequency or intensity of claims. That requires gathering enough accurate information. This task is explored in the next part of this article.

3 - Data

A particularly concerning aspect of emerging (or evolving) risks is the lack of knowledge the insurance sector is faced with. To build efficient coverage strategies, one first needs to know the enemy, and improve how the risk is measured, as pointed out in the recommendations of the Direction Générale du Trésor (2022). The challenge is then to reach a level of knowledge and anticipation that compensates the lack of experience. We have already seen the importance of information for ensuring insurability: uncertainties impact the premiums, discourage some players from entering the market, and, in the end, hold back its development. At the same time, it is crucial that the market grow in order to create this experience.

Insurance companies benefit from a particularly valuable position for learning about a risk: they have the ability to collect data related to the risk from their policyholders. More precisely, data related to claims and their management is particularly precious, since it makes it possible to obtain information about the circumstances and consequences of a risk at an individual level, and to link that to the final cost. However, data about the economic losses resulting from catastrophes is usually difficult to gather. Data gathered policy by policy is more precise than aggregated loss estimations announced publicly following a disaster. An additional interesting aspect is the ability to link this information on claims to exposure data, namely data related to the composition of the portfolio. This knowledge is important since it makes it possible to statistically correct the possible biases of estimates from these databases.

But using this asset efficiently can be challenging, especially when one is in the initial phase of gathering experience on a particular risk. In section 3.1 we first explain the finality of the use of data, by explaining how it can be used to put together projection models, which are essential for the insurance business. To use data, it is of course necessary to gather it, which means structuring a way to obtain and process relevant information. This structuration and industrialization are not necessarily obvious in the case of emerging risks, as we will see in section 3.2. In that case, information is scarce, and it often becomes necessary to rely on expert judgment. We address this question in section 3.3, emphasizing the difficulties in incorporating such judgment in a quantitative measure of the risk and in taking into account the degree of reliability of the experts. Section 3.4 then explores the question of information sharing to increase the quantity of data and to mutually benefit from the experience of the players. Organizing such mutualization of data faces numerous difficulties, starting with the necessity of respecting the competition between insurers. We present some examples of such initiatives, well established or currently being put together.

3.1 Projection models and data

Creating an economic balance around an insurance contract requires anticipating the future number of claims (which are supposed to be absorbed by the total sum of premiums). This requires modelling the (random) outcome of a contract. These models namely describe the probability of a claim occurring (or frequency), and the severity (that is, the cost, but potentially also other kinds of consequences), which is also random. The idea is not to predict at an individual level whether a claim will be made or not (otherwise, insurance would become irrelevant since it is based on individual uncertainty), but to have a relatively clear view at a portfolio level through statistical probabilities.

Based on this analysis, insurers are able to compute requirements from the regulations. The Solvency Capital Requirement (SCR) from the Solvency II directive concerns the amount of reserves that an insurer should keep in order to be almost certain to avoid ruin during the year. The term "almost certain" means that the probability of such an event should be less than 0.5%. One sometimes uses the term of "a 200-year period of returns" to refer to this small probability. Behind this expression, we see the implicit vision of a risk which is supposed, in an ideal world, to be repeated through time without changing. Regulation provides a standard formula to compute SCR, but insurers are encouraged to develop internal modeling that may take into account the specificities of their portfolio and their additional information on the risk. To determine a SCR, one therefore needs to quantify a probability of losses (based on the information one has at a given time) and thus make predictions on the basis of models.

Nevertheless, all these calculations are, in fact, theoretical. Despite their predictive effectiveness in many situations, models are a simplification of reality, and their reliability is sometimes questionable.

First, models depend on parameters. The simplest ones are related to the frequency of claims and the mean value of the claim but knowing just these two indicators does not make it possible to precisely understand the risk, especially when it comes to dealing with very volatile outcomes, and to determine the level of reserves required to survive a non-central scenario that may be of low probability without being unlikely. On the other hand, modern machine learning techniques (also improperly called artificial intelligence) are highly parametrized models that "learn" the values of their parameters from huge amounts of data.

No matter the complexity of the model that is considered, the calibration of its parameters requires information, which means data. Moreover, the more volatile the risk, the more data is usually required to properly refine the models. This is essentially because of two factors:

- volatility, that is uncertainty related to the outcome, is partially caused by the complexity of the risk. Thus, understanding the physical phenomena at stake is difficult to achieve and requires a large quantity of information.
- catastrophes are supposed to be rare, and huge historical databases are required to capture even a small number of such events and learn from them.

This need for data is also increased by the speed with which risk is changing. If risks are changing quickly, one must find clues of what direction they are changing in. These clues have to be found in the past in order to project them into the future. There is no certainty that this past trend will continue (abrupt changes may exist). This is of course a limit to every statistical approach. Nevertheless, even when assuming that the trend will remain stable, projection models require more data in order to be reliable.

It is important to understand that the uncertainty of the projection is paid for by both insurer and policyholder. From a prudential perspective, it increases the SCR. The required volume of reserves grows. Premiums usually reflect this by the introduction of loading factors. To summarize, our inability to correctly understand and model the risk results in a price that deteriorates the economic efficiency of insurance contracts.

Focus 3.1: Effect of lack of data on mutualization

Mutualization is based on the idea that a large number of policyholders absorbs individual uncertainty. But for a given risk, the number of policyholders required to ensure a balance with good confidence depends on several factors. The main one is the volatility of the risk (that is, the uncertainty related to the outcome from an individual perspective).

Lack of data tends to increase this uncertainty. The premium is then based on a prediction of the outcome, which is less reliable, adding some volatility to the result. However, even if data analysis were to lead to a more pessimistic prediction, if the latter is more reliable due to better information, the situation is better - reducing uncertainty makes it possible to better anticipate, with potentially more efficient coverage strategies.

It is important to note that using more data to achieve a better understanding of a risk should not be to the policyholder's disadvantage. The premium paid results from combining a prediction based on an average scenario and a loading factor, which includes a security margin related to the poor quality of information that is used. Even if the "pure premium" (that is the prediction of the average case) is revised and increased due to new data, the outcome may be a win-win situation for both policyholder and insurer thanks to the reduction of the margin related to uncertainty.

3.2 Emerging risks

It is obvious that emerging risks present a particular difficulty. Since they are supposed to be new, historical data on them is scarcer. Depending on the nature of the risk, the whole process of data gathering may be more or less difficult to design. If the nature of the risk is well understood, data pipelines may already exist, and the question is essentially to improve and adapt them. Facing a new threat that was not in the scope of traditional insurance is more challenging. We explore different cases below.

Example 1: Drought. Drought is technically an old risk, but today the risk must be estimated in the context of climate change. Since we are dealing with a meteorologically driven risk, many sources of data have already been organized to collect information and build indexes (like SSWI, see section 2.4). An adaptation of the existing data collection procedure and treatment is still a methodological challenge, but the pipeline for gathering a huge quantity of information already exists.

Example 2: Pandemic. The Covid-19 pandemic gives an example of a progressively growing data collection framework (not driven by insurance perspectives). In the first days of the pandemic, little information was available on the virus, diagnosis techniques were not robust, and data collection was erratic, making any projection of the crisis very uncertain. Progressively, data collection was rationalized and standardized, leading in France to the constitution of the Covid dashboard. Although the appearance of a new virus always creates a new situation, the health sector is organized to gather data and use it to project evolutions. For example, the French Sentinelles network (2022) has been tracking the flu since 1984 and was rapidly adapted to Covid-19, together with the global network of flu surveillance of the WHO (Aranzazu, 2013).

Example 3: Cyber. The situation is different from the two risks above, because there is no tradition of data collection. It is not only a problem of identifying a datastore that could stock the information, but also of understanding which type of information should be collected. Contrary to natural risks or health, there is no clear physical understanding of the important risk factors that need to be watched.

Clearly, the latter situation is the most challenging. A discussion with experts is necessary to know what to check, otherwise important risk factors may be overlooked. Nevertheless, one should not think that the situation is necessarily simple in the first two cases. To take the drought example, the phenomenon of ground swelling showed the importance of the type of constructions that are at risk (the Ministère de la transition écologique (2021) demonstrated that, depending on the type of construction, the probability of making a claim could be significantly higher). This lesson has been learned recently, and the importance of this risk factor made necessary a discussion with housing experts. In other words, untraditional data - not necessarily purely economic - should be mixed with more classical statistics. This type of expertise, precious in the comprehension of the very structure of the risk, may be hard to incorporate, as we will discuss it in the next section.

3.3 Expert judgment

Expert judgment is a natural way to compensate the lack of data. The reliability of these judgments clearly depends on the reliability of the expert, and very few ways exist to control this reliability in absence of data that may be used to confront their expertise with reality.

Another difficulty is the fact that expert judgment may not be optimized for the level of quantitative analysis required by insurance models. For example, cyber scores (Vie publique, 2022) are ways to measure a level of a potential victim's exposure to this risk. But the economic translation of these scores is not obvious and makes it necessary to follow up on these indicators. The difficulty that security experts have in evaluating an economic impact – which is usually far from their scope of expertise – presents an additional challenge.

Therefore, relying on experts should not mean that the question of collecting data has been resolved, at least for two reasons:

- the quality of experts has to be verified
- it is necessary to follow up on the indicators proposed by experts to measure the risk and to identify their precise link with the resulting losses.

Let us also note that actuarial methodologies contain techniques adapted to the progressive addition of data to expert judgment (Bayesian analysis, or credibility theory, see Focus 3.2). These techniques make it possible to progressively shift from a situation where the expert is the sole source of information, to a situation where new data make it possible to combine the unbiased (but rare) historical data of the insurer with expert analysis. The consistency of these techniques implicitly requires an underlying stability of the risk. If its evolution is hard to assess, these procedures may become erratic.

Let us also mention the potential constitution of a reference database for a given risk, which can be assimilated to a special form of expert judgment. A good example are regulatory lifetables: they are the result of a

preliminary statistical analysis for a population that serves as a reference. The tables are usually unable to reflect the mortality of a given insurance portfolio, since the portfolio is the result of a particular (unknown) selection from the total population. This selection has no reason to be representative of average mortality, so the reference table provides biased information. Nevertheless, it can be used to position the portfolio with respect to this reference.

Focus 3.2: Bayesian approach, advantages and limits.

The use of Bayesian analysis for evaluating a risk has a long history. The Bayesian approach has to be compared with the classical frequentist approach.

In a frequentist approach, data is used without pre-conceived information about the risk. To estimate the expected (or average) value of a loss, one gathers historical data on the losses and computes the empirical mean of the past losses. If the database that is used is large enough (and if some kind of stability has been identified in the phenomenon or in its evolution), the value obtained through this process is reliable. However, a small database can lead to errors in evaluations, which may lead to future disappointments regarding the results of the contracts. The term "small" has to be considered in view of the uncertainty - the more volatile a risk is, the more data is required to achieve a better understanding.

On the other hand, the Bayesian approach can be seen as a way to improve the quality of the estimation through the introduction of a prior. This prior can be roughly defined as a preliminary idea on the value(s) one wishes to estimate. For example, if an expert judges the average value of a loss to be close to 100K euros, a Bayesian method will distort the purely frequentist estimation to make it closer to 100K euros. To find the compromise between the frequentist analysis and the prior, Bayesian approaches integrate the reliability of the database (typically, how large is it?), and the degree of confidence in the preliminary expertise.

This approach is appealing, since it can spectacularly improve the prediction of the outcome, without necessarily requiring additional data gathering. The recent report from the French Treasury on cyber insurance indicates that Bayesian analysis is a promising way to get around the lack of data.

But the advantages of Bayesian analysis should not overshadow its important limits. An improved prediction will be reachable only if the prior is good, that is, if the preliminary expertise is accurate. Regarding emerging risks, it may not be simple to obtain expertise, and its reliability can sometimes be questionable when the experts' estimations do not agree. Moreover, the available expertise is not necessarily easy to translate into the quantitative language required to compute insurance premiums and reserves. Hence, calculating a prior can become an delicate job.

In the end, finding the proper prior can, in itself, require data. A good example, in more classical cases, is given by credibility theory. A prior is calculated based on market data (or any other reference), whose analysis is modified using individual historical data (which is scarce). In this situation, the first step is to select the common reference, which may require a major effort for emerging risks.

Focus 3.3: Positioning with respect to a population that serves as reference

Positioning portfolios with respect to a reference is a classical method in actuarial studies. Some similarities with the Bayesian approaches exist in the sense that this introduces external information to supplement the frequentist approach (which is unsuccessful because of a lack of data).

The idea is the following: consider that we have data on losses related to drought in a large part of a country, considered here as a reference. Assume that the related data is sufficiently extensive to properly estimate and anticipate the frequency of claims and the potential associated losses. However, if one is interested in the situation of a specific insurance portfolio, the analysis performed on the reference would provide a biased analysis. The insurance portfolio does not mimic the reference population. Its composition and its geographical distribution are not similar, and the behaviors of the policyholders may be different.

A frequentist unbiased method would be to drop the reference information and to rely only on data coming from our target, that is, from our portfolio. But the size of the portfolio is much smaller than the reference population, and historical data may be more recent.

Positioning a portfolio consists of achieving a compromise between these two extreme approaches (relying on the reference or only on the experience of the portfolio). One assumes that there is a relationship between the two populations (reference and portfolio). Assuming the relationship means considering that the portfolio structurally behaves in a relatively similar way to the reference, but with a degree of freedom that makes it possible to include its specificity.

Identifying this relationship (assuming that this relationship exists) is a much simpler statistical problem, requiring less data. Hence, it is a way to benefit from the quality of analysis of a large population: one population introduces some bias, but the other aims to reduce the difficulties of making an estimate.

These techniques are classically used in mortality analysis, where the lifetable from regulators becomes the reference. Apart from determining whether a simple relationship exists between populations in certain cases, it is a challenge to constantly check whether this relationship tends to be stable over time or not.

3.4 Information sharing

To achieve a proper understanding of the risk, one needs an important quantity of data, and potentially from other fields than insurance (climate data, data on housing, cybersecurity data, epidemiological trends…). Nevertheless, gathering such types of information is difficult:

- first because systematically collecting information on policyholders is hard. The most standard way to proceed is to draft questionnaires. However, some policyholders may find it difficult to fill out the questionnaires (they may not have the knowledge to answer the questions; this is frequent in cyber where CESIN and AMRAE have pointed out this problem). In some cases, it can even dissuade the policyholder from taking out a policy, especially when doubts exist about the ability of the insurer to use it efficiently.

- an insurance company that would keep too much strategic data on its policyholders could become a privileged target for hackers (even if we are not talking about cyber insurance, insurance companies can also be victims), who may want to obtain information on other targets (this danger exists even when one is not talking about cyber insurance).

Artificial intelligence techniques may be a way to (partially) circumvent this issue by retrieving information indirectly from other sources of data: meteorological data, images, or scans of companies performed by cybersecurity firms are a potential means for accessing some of the information. However, these techniques are no miracle solutions and, at the very least, the question of interpretation and confidence in their analysis is complex. Lack of confidence in the projections, in the end, does not help reduce the uncertainties, hence the premiums.

The development of information sharing between insurers seems more effective. The advantage is to reach statistical robustness more rapidly when trying to evaluate the consequences of a risk. In natural disasters, the database SILECC (see Focus 3.4 below) stored by Mission Risques Naturels (MRN) is an example of collaboration between insurers in an attempt to more accurately anticipate risk.

Information sharing does not necessarily prevent competition. It is hard to believe that a single player could benefit from a competitive advantage by simply understanding a risk better than others, in a market where competitors are watching each other and can adapt their prices to the behavior of their competitors. However, a market in which prices do not reflect the risk is particularly dangerous (this situation has been documented in the case of emerging markets, for example (Lester, 2011)).

Cyber risk is a domain for which this question is even more concerning: the malicious part of cyber is driven by humans. The cybercriminal groups make active use of information sharing, which they benefit from significatively when compared to insurance companies if the latter do not want to collaborate among themselves. The insurers' worst enemy is probably not their competitors, but the risk created by hackers who don't care if they don't play by the rules.

On the other hand, there is a danger in information sharing, and critical attention should be paid to one aspect: information sharing should not become or be perceived as collusion, which would be against the law. A clear set of rules should be established for it.

In the case of natural disasters, the example of the French MRN is a good example of successful collaboration of this kind. But its creation required overcoming legal issues like GDPR, and persuading insurers that they could mutually benefit from it. Two arguments can be advanced that probably helped to convince the different stakeholders:

- the provided service: the insurer does not simply transmit data but may expect returns and indicators that help him perform better risk management.
- the fact that the information can also be used (and promoted) as serving the public interest for prevention (for example, MRN participated in a joint study to establish a risk map related to ground swelling (Asensio et al., 2022)). This last point should not be neglected, because it plays an important role in the image of

the insurer with the public and public authorities. That may increase the influence of insurers on changes in regulation and on measures to combat risk.

In the case of cyber risk, the question of gathering information is mentioned by the Direction Générale du Trésor, 2022). The creation of ACYMA (Action contre la CYber MAlveillance, 2019), whose mission is to create an observatory of cyber risk that could be under the supervision of ANSSI, can be the occasion to design a proper way to share and use collective information.

Focus 3.4: Mission Risques Naturels and SILECC database

Mission Risques Naturels is an example of a French association created by the local federation of insurers (France Assureurs) and the association of mutuals insurance companies (GEMA) in the early 2000s. Its goal is to enhance knowledge of natural disaster risks, while contributing to prevention. The association is involved in studies and actions conducted by central administrations. It also follows scientific and foreign initiatives. Among the services proposed by MRN, the association provides a geographic information system to evaluate the exposure to natural risks.

The SILECC database is an example of an information system that gathers claims data from various insurance companies (in 2017, 13 companies, comprising 72% of the market, contributed) and that aggregates data at a level that makes detailed analysis possible without confidentiality being endangering. The richness of this database is a key element for improving the measuring and the understanding of risk.

Conclusion

The conjunction of emerging or evolving risks represents a turning point for insurance. The stability of its model has been put into question by the changes in society and the environment. The question of insurability is crucial and is a challenge for the survival of the entire system. From a solvency point of view, of course - the huge economic cost that can be imagined potentially poses a danger for the reserves of insurance companies. But also, from the perception of the role of insurance in modern societies. Efforts should of course be made to protect solvency through the introduction of safeguard clauses, removing situations that may endanger mutualization from contracts. But exclusion should not be the sole response to the multiple challenges raised by the modern era. Even from a strictly business point of view, failure to face these challenges would reduce the attractiveness of insurance contracts, forcing the public to search for other kind of protections.

But the path to insurability is arduous. To build efficient risk transfer solutions, innovative mechanisms should be developed. None of them constitute a miracle solution, but a careful combination may improve perspectives. Regarding particularly elevated claims, it seems difficult to avoid the discussion on public intervention. But this collaboration should be anticipated and encouraged with the idea of protecting both public finances and the economic stability of the private insurance sector. In particular, public protection can

only be effective if coupled with an active prevention strategy in which all stakeholders (insurers but also policyholders) must pull their weight.

This raises the question of the need to establish efficient sharing of the risk among stakeholders: policyholders, State, and insurance companies. For large corporate risks, a combination of captives and traditional insurance seems to be a way to make the market more fluid by making it possible to deal with very extreme claims, reaching beyond the appetite of insurance companies for this very risky segment of the problem. This combination of self-insurance and outside insurance should not be thought of as the insurance sector giving up, but as a way to develop a positive culture of risk and to progressively learn about how to improve coverage. Self-insurance can also be developed through the creation of mutual insurance ventures by industries from various exposed sectors, like the example of MIRIS for the case of cyber (Ladbury, 2022), which was recently created in order to go beyond the limited insurance capacities offered by the market. In any case, regulation is not homogeneous between European countries and a reflection on how to harmonize and facilitate the harmonious development of such mechanisms should be undertaken. Additionally, the question of allowing smaller companies to have access to such solutions is still open, since this self-insurance principle is essentially reserved for multinationals.

It is therefore essential to look at systems of protection that have proved their effectiveness in protecting industries and individuals. The French "Catastrophes Naturelles" system is certainly a vehicle that will evolve (and has been continuously evolving over the years), but that constitutes an example of relatively harmonious collaboration between the public and private spheres. Its generalization to other types of risks is not necessarily clear (how to define a cyber catastrophe, for instance?), nor is it to other types of environment regulation. However, lessons should be learnt on what could be extended to the European level – faced with the extreme catastrophes that result from the changing environment, the issue of scale can be solved only at the European level, which has the proper dimension to deal with risks that do not acknowledge borders. Otherwise, in the absence of coordination, national protection schemes may be endangered, and there may be distortions between countries if national systems fail.

In any case, all the strategies that can be developed will remain effective only if one knows the enemy. This means gathering enough information to anticipate changes and create financial protection. Insurance companies benefit from a special position in this field of data collecting, since they have the ability to store and process precise economic data. Purely economic data should be enriched with data from other fields (scientific, tech, threat intelligence, construction). This discussion with experts in areas that may not be so close to the financial sector is a real challenge, particularly from the methodological point of view when it comes to transforming these inputs into quantitative measures.

This necessary collaboration in information sharing should also be thought as collaboration between European nations. A system is yet to be built that efficiently collects and processes the information required by the sector to properly analyze and anticipate new risks. Agencies like Eurostat produce valuable indicators on many economic or risk related indexes that are unfortunately insufficient, in terms of precision, for responding to the enormous challenges of understanding, measuring, and fighting risk. As pointed out in Part III of this paper, aggregated information does not make the detailed analysis essential for reducing uncertainty. The most pertinent type of information is probably more to be found in data stored by private entities (industries, insurance) than in national statistics. The European public sector can play a key role in

organizing this information sharing between all those concerned by the risk, respecting privacy, competition, and defense (due to the extreme sensitivity of some information because of the vulnerability of entire economies).

The extreme severity of the risk that we now face makes this effort of collaboration (within sectors and with the others concerned by risk) essential for pushing back the boundaries of insurability.

Bibliography

Agence Nationale de la Sécurité des Systèmes d'Information (2020), *État de la menace rançongiciel à l'encontre des entreprises et institutions*, 5 février, https://www.cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/.

Aranzazu A. (2013), Le réseau mondial de surveillance de la grippe de l'OMS. Modalités de circulation des souches virales, des savoirs et des techniques, 1947-2007, Sciences sociales et santé 2013/4 (Vol. 31), p 41-64 https://www.cairn.info/revue-sciences-sociales-et-sante-2013-4-page-41.htm#:~:text=1Le%20programme%20de,En%201978%2C%20le%20Syst%C3%A8me%20mondial.

Asensio C., Bouveret A. & Harris A. (2022), Financial stability risks from cloud outsourcing, ESMA Working Paper No. 2, https://www.esma.europa.eu/sites/default/files/library/esma_wp_cloud_may_2022.pdf.

Association pour le Management des Risques et des Assurances de l'Entreprise (2022), LUCY : LUmière sur la CYberassurance, juin, https://www.amrae.fr/bibliotheque-de-amrae/undefined.

Bafoil F. (2022), Chroniques des tempêtes (2/2) La tempête Alex, un an après, Blog de la Caisse des Dépôts.

Barry L. (2020), L'invention du risque catastrophes naturelles, *Chaire Pari*, https://www.chaire-pari.fr/wp-content/uploads/2020/02/Catastrophes-naturelles-invention-dun-risque-WP.pdf.

Bloomberg (2020), How pandemic bonds became the most controversial investment, December 9, https://www.bloomberg.com/news/features/2020-12-09/covid-19-finance-how-the-world-bank-s-pandemic-bonds-became-controversial?leadSource=uverify%20wall.

Broberg M. (2020), Parametric loss and damage insurance schemes as a means to enhance climate change resilience in developing countries, *Climate Policy*, *20*(6), 693-703.

Caisse Centrale de Réassurance (2016), La crue de la Seine en Ile-de-France, mars, https://www.ccr.fr/documents/35794/35839/CCR-Rapport+Crue+Seine.pdf/0785a783-ff35-4431-983b-ee0ff704f12a?t=1496834508000.

Chowdhury P., Paul S. K., Kaisar, S. & Moktadir M. A. (2021), COVID-19 pandemic related supply chain studies: A systematic review, *Transportation Research Part E: Logistics and Transportation Review*, *148*, 102271.

Conseil Économique, Social et Environnemental (2022), Climat, cyber, pandémie : le modèle assurantiel mis au défi des risques systémiques, https://www.lecese.fr/sites/default/files/pdf/Avis/2022/2022_07_risques_emergents_systeme_assurantiel.pdf

Copernicus (2022), Summer 2022 Europe's hottest on record, 8 September, https://climate.copernicus.eu/copernicus-summer-2022-europes-hottest-record#:~:text=August%202022%20was%20generally%20much,with%20extreme%20winds%20and%20rainfall.

Cyber malveillance (2019), Qui sommes-nous ?, 27 novembre, https://www.cybermalveillance.gouv.fr/tous-nos-contenus/a-propos/qui-sommes-nous.

Direction Générale du Trésor (2022), *Le développement de l'assurance cyber*, septembre, https://www.tresor.economie.gouv.fr/Articles/00367730-14c0-4303-95af-eeb6442fb19b/files/8a344142-fcd5-4d21-a3d7-abb0a404087f.

Eaton C., & Volz D. (2021), Colonial Pipeline CEO tells why he paid hackers a $4.4 million ransom, May 19, *Wall Street Journal*.

Faure-Muntian V. (2021), *La cyber assurance*, Rapport du Groupe d'Études Assurance de l'Assemblée nationale, octobre, https://www.valeriafauremuntian.com/_files/ugd/50f22c_361ca4c49de74364b3ff2058441fd0a7.pdf

Fekete A. & Sandholz S. (2021), Here comes the flood, but not failure? Lessons to learn after the heavy rain and pluvial floods in Germany 2021, Water, 13(21), 3016.

Ferland J. (2019), Cyber insurance–What coverage in case of an alleged act of War? Questions raised by the Mondelez v. Zurich case, *Computer Law & Security Review*, *35*(4), 369-376.

France Assureurs (2020), France Assureurs précise son projet « CATEX », 26 novembre, https://www.franceassureurs.fr/nos-positions/lassurance-qui-protege/projet-catex/.

Grandell, J. (2012). Aspects of risk theory. Springer Science & Business Media.

Haut Comité Juridique de la Place Financière de Paris (2022), *Rapport sur l'assurabilité des Risques Cyber*, 28 janvier, https://www.banque-france.fr/sites/default/files/rapport_45_f.pdf.

Horton J. B. (2018), Parametric insurance as an alternative to liability for compensating climate harms, *Carbon & Climate Law Review*, *12*(4), 285-296.

Institut des Hautes Études pour la Défense Nationale (2020), Citoyens et institutions à l'épreuve d'une atteinte majeure à la défense et à la sécurité nationale à la suite d'événements climatiques d'ampleur, https://ihedn.fr/wp-content/uploads/2021/06/IHEDN-72e-SN-POLDEF-C1.2-Note-operationnelle.pdf.

Institut Montaigne (2019), Like a Hurricane: Preparing for a Large Cyber Attack, Analyses, January 21, https://www.institutmontaigne.org/en/analysis/hurricane-preparing-large-cyber-attack.

Johnson L. (2021), Paying ex gratia: Parametric insurance after calculative devices fail, *Geoforum*, *125*, 120-131.

Ladbury A. (2022), Leading European multinationals create cyber mutual to counter capacity crunch, Commercial risk, September 9, https://www.commercialriskonline.com/leading-european-multinationals-create-cyber-mutual-to-counter-capacity-crunch/.

Lallie H. S., Shepherd L. A., Nurse J. R., Erola A., Epiphaniou G., Maple C. & Bellekens X. (2021), Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic, *Computers & Security*, *105*, 102248.

Latruffe L. & Picard P. (2005), Assurance des catastrophes naturelles : faut-il choisir entre prévention et solidarité ?, *Annales d'économie et de statistique*, 33-56.

Lester R. (2011), The Insurance Sector in the Middle East and North Africa, The World Bank Middle East and North Africa Region Financial and Private Sector Development Unit, Policy Research Working Paper 5608, March, https://documents1.worldbank.org/curated/en/191531468110930768/pdf/WPS5608.pdf.

Lloyds (2018), Pandemic, potential insurance impacts, https://assets.lloyds.com/media/3066455e-3231-46a7-9dea-e5c62bfaaf2d/pdf-pandemic-potential-insurance-impacts-er-pandemic-insuranceImpacts-v2.pdf.

Lloyd's London (2022), *State backed cyber-attack exclusions,* Market Bulletin 16 August.

Lopez O. & Thomas M. (2022), Parametric insurance for extreme risks: the challenge to properly cover severe claims, https://hal.sorbonne-universite.fr/hal-03524677/

Mantha B. R., & García de Soto B. (2021), Cybersecurity in Construction: Where Do We Stand and How Do We Get Better Prepared, *Frontiers in Built Environment*, 43.

Martínez J., & Durán J. M. (2021), Software supply chain attacks, a threat to global cybersecurity: SolarWinds ' case study, *International Journal of Safety and Security Engineering*, *vol*, *11*(5), 537-545.

Ministère de la transition écologique (2021), Cartographie de l'exposition des maisons individuelles au retrait-gonflement des argiles, juin,
https://www.statistiques.developpement-durable.gouv.fr/sites/default/files/2021-06/note_methode_croisement_retrait_gonflement_argiles_juin2021v3.pdf

Ministère de l'intérieur (2022), projet de loi d'orientation et de programmation, 7 septembre, https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000046266613/?detailType=CONTENU&detailId=1

Mission Risques Naturels (2019), Mise à l'enquête publique – Nouvelle carte de susceptibilité RGA, 19 avril, https://www.mrn.asso.fr/mise-a-lenquete-publique-nouvelle-carte-de-susceptibilite-rga/.

National Association of Insurance Commissioners (2020), *Report on the Cybersecurity Insurance Market,* https://www.insurancejournal.com/app/uploads/2021/11/NAIC-Cyber_Insurance-Report-2020.pdf.

Pastré O. & Albouy F. (2021), L'avenir de la réassurance post-Covid, *Notes stratégiques de l'Institut Choiseul,* https://www.choiseul-france.com/wp-content/uploads/2021/06/Notes-Strat%C3%A9giques-R%C3%A9assurance-vdef.pdf

Poullennec S. (2021), *Covid : AXA transige avec 80 % de ses clients restaurateurs,* Les Echos, 18 novembre,

https://www.lesechos.fr/finance-marches/banque-assurances/covid-axa-transige-avec-80-de-ses-clients-restaurateurs-1364935.

Schwarcz S. L. (2008), Systemic risk, *Geo. Lj*, *97*, 193.

Sentinelles (2022), Situation observée en France métropolitaine pour la semaine 49 de l'année 2022, du 05/12/2022 au 11/12/2022, 14 décembre, https://www.sentiweb.fr/.

Smilyanets D. (2021), 'I scrounged through the trash heaps… now I'm a millionaire:' An interview with REvil's Unknown, The Record, March 16, https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/.

Soubeyroux J.-M., Kitova N., Blanchard M., Vidal J.-P., Martin E. & Dandin P. (2012), Sécheresses des sols en France et changement climatique : Résultats et applications du projet ClimSec, *La Météorologie*, 78, 21-30.

Tourny È. (2017), Cyber sécurité et attaques informatiques : les leçons à tirer de Wanna Cry et Not Petya, *Paix et sécurité européenne et internationale*, (7).

Tsvetanov T., & Slaria S. (2021), The effect of the Colonial Pipeline shutdown on gasoline prices, *Economics Letters*, *209*, 110122.

Vidal J.-P, Wade S. (2009), A multimodel assessment of future climatological droughts in the United Kingdom, International Journal of Climatology, 29(14), 2056-2071.

Vie publique (2022), Loi du 3 mars pour la mise en place d'une certification de cybersécurité des plateformes numériques destinée au grand public, https://www.vie-publique.fr/loi/282626-loi-3-mars-2022-cyberscore-securite-des-plateformes-numeriques.

Zhongming Z., Linong L., Xiaona Y., Wangqiang Z., & Wei L. (2022), AR6 Synthesis Report: Climate Change, Intergovernmental Panel on Climate Change (IPCC).