Maîtrise du Risque Cyber et Assurance : Scénario cyber s'appliquant à la filière aéronautique

Philippe Cotelle, Philippe Wolf, Bénédicte Suzan, Jean-Laurent Santoni, Laurence Lemerle, Christophe Delcamp, Virginie Wyka, Sébastien Héon

LA MAÎTRISE DU RISQUE CYBER SUR L'ENSEMBLE DE LA CHAÎNE DE SA VALEUR ET SON TRANSFERT VERS L'ASSURANCE
Scénario cyber s'appliquant à la filière aéronautique
Réponse du marché

RÉSULTATS de la RECHERCHE

Année 3 : Séminaire février 2018 - février 2019

RAPPORT ÉTABLI PAR

Philippe Cotelle Insurance Risk Manager in charge of Cyber Risk for AIRBUS	Philippe Wolf Project Manager EIC IRT SYSTEMX	Bénédicte Suzan R&T Innovation Cooperation AIRBUS Defense and Space
Groupe de travail des courtiers Jean-Laurent Santoni CleverCourtage	**GT Cyber FFA** Laurence Lemerle, AXA Christophe Delcamp, FFA	**Sous-Commission Cyber APREF** Virginie Wyka, PARTNER RE Sébastien Héon, SCOR

EN PARTENARIAT AVEC

POUR TOUT RENSEIGNEMENT CONCERNANT CE RAPPORT, VOUS POUVEZ CONTACTER L'IRT SYSTEMX AUX COORDONNÉES SUIVANTES : IRT SystemX, 8, avenue de la Vauve, CS 90070 – 91127 Palaiseau Cedex
Site internet : www.irt-systemx.fr ; Courriel : philippe.wolf[at]irt-systemx.fr

Table des matières

Liste des illustrations

I. Présentation des travaux

Dans le cadre de son projet EIC[1] (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité), l'IRT SystemX mène des travaux sur **la maîtrise du risque cyber** dans une approche pluridisciplinaire croisant sciences mathématiques et informatiques avec sciences économiques, sociales et du comportement.

Sous l'impulsion du *Chief Security Officer* d'**AIRBUS** et du Directeur général de l'**ANSSI** (Agence nationale de la sécurité des systèmes d'information), l'IRT SystemX anime depuis novembre 2015 un groupe de travail sur « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». Il réunit des spécialistes de l'assurance et de la réassurance, des courtiers, des juristes, des actuaires, des industriels (*Insurance Risk Managers*), des experts de l'OCDE, sous l'égide de la Fédération Française de l'Assurance (FFA), de l'association française des professionnels de la réassurance en France (APREF), de l'association française des professionnels de la gestion des risques et des assurances (AMRAE) et de *The Federation of European Risk Management Associations* (FERMA).

Un **premier rapport de recherche[2]** a été rédigé et publié fin juillet 2016 (en français et en anglais).

L'année 1 de la recherche s'est organisée entre des réunions plénière et des réunions de préparation. Le rapport et les recommandations montrent l'importance de conduire une quantification financière du risque cyber en interne de l'entreprise, de définir un référentiel et un langage commun aux différentes parties prenantes, d'établir de nouvelles règles de communication entre elles (la question de la confidentialité a contribué à la mise en place de la plateforme cybermalveillance ACYMA[3] dont la FFA est partenaire pour une meilleure compréhension de l'exposition et des sinistres, du support à apporter aux entreprises qui subissent des pertes) et de développer une meilleure connaissance des couvertures d'assurance (voir la matrice). Cette question a été reprise depuis dans le cadre du rapport du Club des juristes (mieux comprendre et appréhender les couvertures cyber)[4] et sous une forme améliorée par l'OCDE[5]. Les travaux ont également mis en évidence le poids des *silent covers*, ou couvertures non affirmatives. Un sujet sur lequel la profession s'est penchée depuis. Les travaux de recherche aident ainsi à construire la branche qui est en train de se développer. Quant au manque de définition et de qualification juridique de la donnée, le droit se développe moins vite que la technologie et ses usages.

Quelques-unes de ces recommandations ont été reprises dans la Stratégie de cyberdéfense du SGDSN publiée en mars 2018 et notamment les conditions de la confidentialité sur les attaques cyber[6].

---

[1] Voir https://www.irt-systemx.fr/project/eic/

[2] Voir http://www.irt-systemx.fr/publications/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/

[3] https://www.cybermalveillance.gouv.fr/

[4] https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_assurer-le-risque-cyber_janvier_2018_fr.pdf

[5] https://www.oecd.org/pensions/The-cyber-insurance-market-responding-to-a-risk-with-few-boundaries.pdf

[6] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

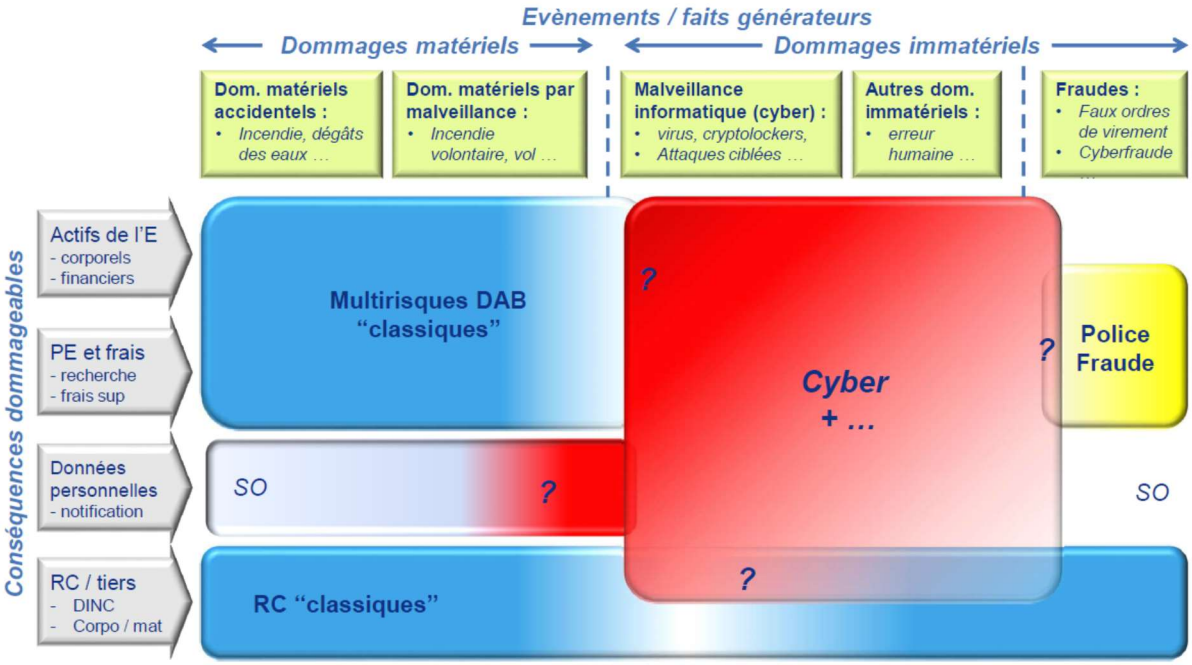


Figure 1 - Matrice synthétique Faits générateurs dommageables / Garanties

Le **deuxième cycle de séminaires** en 2017 a traité principalement de **la valorisation des données intangibles conditions nécessaires pour connaître, gérer et maitriser le risque cyber pour ensuite le transférer éventuellement vers l'assurance**. Un **deuxième rapport de recherche** a été publié en janvier 2019[7]. Ce rapport[8] a été rédigé et publié en français et en anglais.

L'année deux de la recherche a porté sur un sujet ambitieux, le transfert vers l'assurance des biens intangibles. Depuis lors, d'autres rapports ont adressé le sujet sur la valorisation des biens intangibles des entreprises. Un sujet pour lequel il est encore difficile d'apporter des réponses mais qui est stratégique pour l'avenir de la gouvernance du risque cyber.

Un certain nombre d'intervenants extérieurs ont apporté un éclairage comme des agences de notation, des auditeurs, des assureurs et des chercheurs pour aider à comprendre comment ils contribuent à la valorisation de l'organisation concernant le risque cyber. La valorisation financière des entreprises prend, en effet, de plus en plus en compte la valeur intangible de leurs données – le patrimoine informationnel. Ceci constitue un véritable retournement de paradigme car il y a 20 ans, selon l'OCDE, 75% de la valeur des entreprises était tangible, aujourd'hui, les chiffres sont inversés. La valorisation de l'entreprise est essentiellement constitutive des biens intangibles. Ces derniers sont par définition plus sensibles au risque cyber, telles les données et la réputation.

Les agences de notation ont présenté comment le risque cyber faisait partie de leur appréciation de la qualité du risque d'une entreprise dans la mesure où si sa valorisation est à risque, ce risque cyber est peut-être un élément pris en compte. La réponse est oui, sous la pression notamment des investisseurs, parce qu'ils ont besoin de cette information qui va leur permettre de prendre en compte la décision d'investissement dans le temps. Et en même temps, les agences ont mis en évidence les problèmes de modélisation. En ce sens, les problématiques des assureurs sont proches de celles des agences de notation.

[7] Ibid.

[8] https://www.irt-systemx.fr/wp-content/uploads/2019/01/ISX-EIC-transfert-risque-an2.pdf

Des avocats ont été interrogés pour comprendre quelle est la conséquence pour les dirigeants sur leur exposition au risque cyber : est-ce que cet élément les expose eux personnellement en tant que mandataire social ? Des chercheurs ont également contribué à la question de savoir s'il est possible de valoriser financièrement ces biens intangibles et s'il est possible d'associer une valeur financière à une donnée hors de la marque et de la propriété intellectuelle. L'étude de décisions de justice a permis de donner des appréciations financières en termes de pertes de données intangibles. L'évolution des normes comptables un enjeu de négociation internationale – l'IFR 48 a récemment exclu les biens intangibles. Un socle théorique et intellectuel permettant d'avancer sur ces questions n'existe pas aujourd'hui mais des travaux sont en cours.

Les travaux menés au sein de l'IRT SystemX doivent contribuer à mieux appréhender les enjeux du risque cyber pour les TPE et PME. La question est prégnante pour les startups dont la valeur est constituée par leur innovation et leur recherche. Si cette information est compromise, c'est la valeur de la société qui est affectée. La question de la protection de l'innovation et du développement de l'économie du futur de plus en plus digitalisée est majeure. Outre la question de la valorisation de la donnée, se pose désormais celle de la valorisation de la connaissance : la problématique de l'intelligence artificielle, l'éthique des algorithmes, la responsabilité des robots et la personnalité juridique des systèmes embarqués, de l'*automotive*, des avions connectés sans pilotes. De nombreuses questions sont ouvertes.

L'assurance et la réassurance constatent ce défaut de valorisation financière des biens intangibles.

Les conclusions de cette seconde année ont peut-être été moins constructives en termes de livrables sur la réponse du marché de l'assurance dans sa capacité à assurer les biens intangibles mais elles ont permis de lancer des réflexions entre assureurs et réassureurs sur l'opportunité ou pas de contrats indiciels, paramétriques.

Les recommandations de la seconde année des travaux portent sur la nécessité d'une mise en place, en interne des organisations, d'une gouvernance du risque cyber et d'une capacité à définir en interne le besoin de couverture – voir également les travaux de FERMA[9] et ceux conduits avec *Insurance Europe*[10]. Le cadre de la communication externe des entreprises sur leur exposition au risque cyber devient un élément important.

La quantification du risque cyber a également besoin d'un cadre normé pour pouvoir comparer le niveau de maturité cyber et le niveau de gouvernance des organisations entre elles dans leurs analyses de risque et pour la quantification de leurs scénarios. Il s'agit de s'entendre sur la prise en compte de la phase de risque, de remédiation et de vigilance dans leurs appréciations. Il faut que les entreprises puissent communiquer sur des statuts d'exposition issus d'un référentiel commun afin que les acteurs de la valorisation des entreprises puissent comprendre et comparer une entreprise par rapport à une autre de manière raisonnable.

Sur les obligations et responsabilité des dirigeants dans le cadre de leur police D&O et leur police cyber, l'existant des couvertures est actuellement positif et il serait opportun de maintenir ce statut.

Concernant l'évaluation financière d'un impact sur les biens intangibles, des progrès sont à conduire mais la tendance est là poussée, à la fois, par les entreprises dès lors que les agences de notation et leurs investisseurs les interrogent sur la manière dont la valeur est protégée. Pour les assureurs, clairement un champ nouveau s'ouvre sur la protection des biens intangibles dans une économie de plus en plus digitalisée.

---

[9] https://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy

[10] https://www.insuranceeurope.eu/sites/default/files/attachments/Preparing%20for%20cyber%20insurance.pdf

Dans les débats sur les défis de l'assurance cyber, l'accès aux données, le risque d'accumulation, la problématique de la modélisation, le problème des couvertes silencieuses ou non affirmatives ont été mise en évidence.

Les réflexions de l'année 3 ont porté sur **la conception et la réalisation d'un exercice cyber s'appliquant à la filière aéronautique** selon une démarche proche de celle développée par l'Université de Cambridge ou des exercices cyber nationaux et internationaux (Piranet, Cyber Europe, Cyber Storm…). L'objectif était de réfléchir autour du concept d'Entreprise étendue et de s'interroger sur le fait, qu'aujourd'hui, une organisation doit être en mesure d'apprécier le risque cyber au long de sa chaine de la valeur et de sa chaine d'approvisionnement pour laquelle l'élévation du niveau de maturité en cyber sécurité est un enjeu stratégique.

Le point de départ de nos réflexions a été l'initiative prise par *BoostAerospace* – Entreprise étendue (**voir annexe 1**), la plateforme d'échanges sécurisée pour les fournisseurs de la filière aéronautique qui souhaite mettre en place des standards de cyber sécurité techniques Bronze, *Silver*, *Gold* adaptés à la filière. Le principe d'une telle démarche est également partagé par l'AMRAE qui estime que c'est moins au régulateur d'imposer des standards techniques et de gouvernance de cyber sécurité de haut niveau qu'aux industriels qui connaissent leurs besoins. En regard de l'initiative de *BoostAerospace* d'élever le niveau des investissements en cyber sécurité, l'opportunité est réelle de mettre en évidence un besoin de couverture cyber pour l'ensemble de la chaine d'approvisionnement. Il est en effet réaliste de penser pouvoir faire correspondre les standards techniques à un besoin de couverture et de développer dans le futur des couvertures en miroir. Il est réaliste de penser, qu'à moyen terme, des sous-traitants Bronze, *Silver* ou *Gold* puissent en tant que tels communiquer avec des assureurs qui reconnaitraient ces standards. Comprenant ce dont il ressort, les assureurs, seraient mieux à même de proposer une couverture adaptée.

L'exercice dans son ensemble permet d'apprécier la résilience de la chaîne d'approvisionnement face au risque cyber en montrant le coût économique d'un scénario catastrophique et en le comparant aux montants financiers qui sont assurés et réassurés.

Les estimations chiffrées permettent de présenter à l'ANSSI une première quantification financière d'un scénario catastrophe affectant une filière industrielle. Elles permettent également aux intégrateurs finaux de l'aéronautique de mieux appréhender l'exposition au risque cyber de la filière, quels en sont les impacts pour les entreprises de rang 1, pour les sous-traitants et de mettre ainsi en évidence la dimension d'une exposition dont ils n'ont, peut-être pas, une connaissance claire. Elles offrent aux courtiers, aux assureurs et réassureurs une meilleure compréhension des enjeux de la résilience cyber de la filière aéronautique.

Le scénario catastrophe n'inclut pas la quantification des conséquences financières de l'attaque sur l'avionneur donneur d'ordre, même si nous en donnons une estimation pour les seuls besoins de l'exercice[11].

[11] Voir https://www.aerotime.aero/clement.charpentreau/22586-boeing-estimates-the-cost-of-737-max-grounding-at-1-billion

II. Démarche de la recherche

Le présent rapport détaille les résultats de la démarche de recherche décrite ci-après.

II.1. Déroulement de la recherche

Les séminaires se sont organisés autour du calendrier suivant :

Sept réunions préparatoires ont été nécessaires pour rédiger le scénario support de l'exercice avec les sachants du secteur de l'aéronautique (*Insurance Risk Managers* d'Airbus, Safran et Thales), des experts cyber, des experts de l'ANSSI, les *Chief Information Security Officer* d'Airbus et de *BoostAerospace*, en présence de RSSI d'entreprises partenaires de *BoostAerospace* (la RSSI de Latécoère, le RSSI d'ERAMET), de la Fédération Française des Assurance (FFA), de la réassurance et des experts en cyber sécurité et d'un représentant du *General Procurement d'Airbus*.

Le scénario qualifié et quantifié a été présenté aux acteurs du marché de l'assurance : courtiers, assureurs et réassureurs lors de la séance d'ouverture des travaux.

Une alternance de séances plénières et par comités professionnels fermés a rythmé l'exercice de recherche pour cette année 3 de façon à ce que chaque séance plénière permette, aux comités qui présentaient leur travaux, de partager leurs réflexions et leurs conclusions.

Le comité courtiers s'est réuni une fois dans le cadre du séminaire IRT SystemX.

Le comité assurance s'est réuni deux fois dans le cadre du séminaire IRT SystemX. Les conclusions ont été préparées dans le cadre du Groupe de travail cyber de la FFA. Lequel s'est réuni en interne FFA à 3 reprises. Une enquête a été également conduite auprès des membres de la Fédération.

Le comité réassurance s'est réuni une fois dans le cadre du séminaire IRT SystemX. La sous-commission cyber de l'Association des Professionnels de la réassurance en France (l'APREF) s'est réunie en interne APREF à 5 reprises pour répondre aux questions posées.

Une réunion supplémentaire du séminaire IRT SystemX a réuni les deux groupes de travail FFA et APREF qui avaient organisé auparavant une réunion commune à leurs deux groupes de travail.

Le séminaire s'est conclu par une réunion finale pendant laquelle, courtiers, assureurs et réassureurs ont présenté les éléments saillants de leur réponse au scénario. La réunion conclusive a synthétisé les enseignements obtenus et préparé les recommandations (**voir chapitre IV**.)

II.2. Finalité de l'exercice

Il s'agit de tester le scénario (**voir chapitre V**.) de risque cyber sur l'ensemble de la chaine de la valeur depuis les fournisseurs jusqu'à l'intégrateur final dans le domaine industriel de l'aéronautique.

Cinq objectifs principaux sont poursuivis :

1. Comprendre l'ampleur du scénario du point de vue du *Insurance Risk Manager*, le qualifier et le quantifier financièrement.
2. Etudier la réponse du marché de l'assurance cyber (**courtiers — chapitre VI**., **assureurs — chapitre VII**., **réassureurs — chapitre VIII**.) en termes de couverture du risque pour tous les acteurs de la filière : depuis les ETI (entreprises de taille intermédiaire) jusqu'aux grands groupes.

3. Quelles couvertures assurantielles répondraient à cet exercice ?
4. Comment les réassureurs géreraient leurs accumulations ?
5. Identifier les domaines assurables et non assurables qui laissent à la charge de la filière des risques non assurables résiduels pour lesquels elle doit s'organiser.

II.3. Conclusions de l'exercice

Nota Bene:

Les chapitres VI, VII et VIII, décrivant la réponse du marché de l'assurance cyber, sont plus techniques. Nous avons préféré conserver dans ce rapport l'ensemble des facteurs étudiés et pris en compte au détriment d'une rédaction plus achevée. En particulier, les omissions (par exemple, recours potentiels des compagnies aériennes) sont notées.

Ces résultats démontrent la faisabilité d'une analyse fouillée sur un scénario qui se veut réaliste[12] et préfigurent de nouvelles méthodes qui sont encore en phases de co-construction entre l'ensemble des acteurs.

[12] Comme le démontre, par exemple, l'information suivante du vendredi 3 mai 2019 : *50 000 entreprises utilisent un logiciel SAP vulnérable*, voir https://www.zdnet.fr/actualites/50-000-entreprises-utilisent-un-logiciel-sap-vulnerable-39884273.htm

III. Résumé des résultats de la recherche

Les travaux ont cherché à quantifier dans le scénario d'attaque cyber retenu sur les acteurs de la chaine d'approvisionnement de l'aéronautique quel pourrait être l'impact assuré pour l'ensemble de la filière aéronautique. Nous n'avons pas, à ce stade, de chiffre crédible sur l'impact économique – les coûts économiques directs et indirects agrégés qui viendraient au-delà de cet impact assuré. Notre estimation ne représente donc qu'une portion de l'impact économique réel subi par la filière.

Dans ce scénario, au regard de nombreuses hypothèses qui seront détaillées par la suite, les chiffres montrent un impact financier sur les contrats d'assurance des sous-traitants du donneur d'ordre (sans évaluation du coût pour ce dernier) de l'ordre de 400M euros[13]. Ce montant correspond à la mobilisation des contrats d'assurance de 11 % des sous-traitants de l'avionneur. Ce montant ne tient pas compte des conséquences sur les autres filières économiques pour lesquelles les sous-traitants travaillent également.

Par ailleurs, la réassurance estime que près de 80% du montant assuré serait effectivement porté par la réassurance. Elle est financièrement en mesure de répondre au sinistre. Cependant, si la réassurance devait payer un tel sinistre au niveau de la filière, selon une prime moyenne estimée à 5 000€ pour les 1800 entreprises du scénario pour un montant de prime totale estimé à 9M€, la période de retour induite serait de 46 ans bien qu'un tel scénario apparait avoir une probabilité de survenance bien supérieure (1 fois tous les 46 ans). Le montant des primes affectées au risque cyber semble donc encore insuffisant pour répondre à des évènements d'ampleur.

Il ressort de cette étude que la réassurance dispose d'un vrai levier pour effectivement contribuer au développement du marché de l'assurance cyber puisque les réassureurs sont ceux qui portent, au final, le risque d'un scénario catastrophique cyber : la gestion des cumuls est, pour eux, un problème particulièrement important. Face aux assureurs cyber qui sont en direct ce sont les réassureurs qui offrent, en effet, les moyens financiers ultimes de fournir les couvertures qui seront déclenchées par les assurés.

Les réassureurs et les assureurs ont également particulièrement mis en évidence le problème de la définition de l'évènement nécessaire à la mise en place de contrats de réassurance des évènements systémiques. Un évènement cyber n'étant pas limité dans le temps, l'espace, ses causes et ses cibles pouvant être variées, il est actuellement compliqué de le qualifier. Ils recommandent ainsi de travailler sur une définition robuste et reconnue de l'évènement cyber catastrophique. L'analogie avec la définition d'un évènement naturel catastrophique, où chaque ouragan, tremblement de terre… est clairement identifié permettant l'application des couvertures de manière non discutable n'est pas opérante pour le cyber.

Les réassureurs pointent aussi le risque de clash entre les différentes solutions de réassurance qui entraine un cumul difficilement identifiable et donc non maîtrisé des sinistres cybers portés par la réassurance. Entre les différents traités Quote-Part et *Excess* par risque ainsi que par type de nature de traités, qu'ils soient des traités de réassurance cyber spécifique ou de garantie plus traditionnelle, la gestion des expositions et des cumuls est une vraie problématique pour la réassurance. Une clarification et une meilleure identification de ces mécanismes de reversement de l'exposition cyber dans le cadre des traités sont donc recommandées. Cet effort doit porter sur les couvertures silencieuses existantes ou non affirmatives ainsi que sur les couvertures cyber dans le cadre de polices non cyber.

Ils alertent enfin sur le problème de tarification au regard du risque cyber : le volume actuel de la prime cyber – phénomène marché – paraît effectivement trop faible par rapport aux enjeux posés par la menace cyber et le besoin

[13] Nous utilisons le symbole M pour million dans ce rapport et le symbole Md pour milliard

de mutualisation du risque – le volume de prime pour la France en 2018 se situe autour de 80M€ (2 700 M€ ou 2,7Md€ pour les États-Unis)[14].

De son côté, l'assurance a mené une double analyse autour des couvertures à proposer à la filière organisées par paquet de garantie et la quantification de cette couverture ? Les assureurs ont identifié les garanties qui pouvaient être mobilisées sur les segments PME et ETI – l'organisation des garanties étant différentes selon les sociétés d'assurance par paquet d'assurance : Paquet 1 – la gestion de la crise : reconstitution des pertes de données, frais de gestion de crise, frais de reconfiguration des systèmes, assistance informatique, recherche de cause ; Paquet 2 – les garanties liées aux pertes d'exploitation et assimilées : PE, pertes immatérielles suite à la remise en question de l'agrément, frais liés à la perte d'agrément et à la nouvelle demande d'agrément, remboursement des pénalités contractuelles ; Paquet 3 – les garanties liées à la rançon : paiement et ou frais de mis en œuvre. Paquet 4 – les garanties liées aux carences : carences de fournisseurs suite à un évènement cyber chez un tiers et ou carence du client suite à un évènement cyber chez un tiers. Les réflexions n'ont pas porté sur les frais de notifications, les pénalités administratives et les biens intangibles.

L'assurance, dans ses analyses, montre que pour la partie RC – responsabilité civile, les couvertures sont non seulement faibles en termes de montant mais se pose de plus la question de la pertinence d'un recours en RC en matière de sinistre cyber. La problématique des mises en causes croisées des acteurs – le fait que les fournisseurs puissent être tiers entre eux ont été écartées de la réflexion. Néanmoins, un travail de réflexion doit être poursuivi afin d'étudier la chaine des responsabilités, les recours possibles entre des fournisseurs entre eux en cas de non-respect d'une obligation de moyen de sécurité en regard des standards de sécurité de *BoostAerospace*, par exemple. L'assurance s'interroge, en effet, sur la capacité de recours, avec succès, des assurés dans le cas d'un défaut de cyber sécurité au titre de la responsabilité civile. Dans la mesure où la sécurité n'est qu'une obligation de moyen et pas de résultat, il reste incertain qu'un défaut de sécurité puisse aboutir à ce que la responsabilité d'un fournisseur soit mise en cause tant au regard de l'état de l'art technique, de maturité cyber ou de standards non encore posés, reconnus et partagés par les différents acteurs aujourd'hui. Enfin, l'appréciation laissée aux juges se prend dans un délai long ; le temps judiciaire n'est pas adapté au temps économique. La recommandation est de mieux prendre en compte le cadre du recours en responsabilité civile pour mieux comprendre le risque juridique financier de l'exposition en responsabilité du fait d'un défaut de sécurité au sein de la chaine d'approvisionnement de l'aéronautique.

En termes d'analyse du risque, de tarification et de qualité du risque, les assureurs mettent en avant leur compréhension encore limitée du risque cyber. Ils ne disposent pas, à ce stade, de toutes les informations nécessaires et pertinentes pour leur profession afin d'analyser la qualité du risque des assurés. Les assureurs recommandent le développement de leurs modèles d'évaluation du risque cyber et de leur capacité à obtenir plus d'information de la part des assurés.

Les courtiers, dans le cadre de ces travaux, ont réfléchi aux propositions qui peuvent être faites que ce soit dans le cadre de polices individuelles souscrites par l'ensemble des entreprises de la sous-traitance ou bien dans celui d'une souscription de polices cadre qui seraient souscrites par les donneurs d'ordre au bénéfice de la filière tout en mettant en évidence l'enjeu de capacité, notamment dans le cas d'une police cadre. Le sujet individuel et collectif n'est pas indissociable. Un socle commun et une approche mutualisée collective peuvent être combinés. Les réflexions ont également porté sur les options possibles de contrat individuel, contrat collectif ou pour compte ainsi que la rédaction d'un *wording* adapté et partagé par les assurés de la filière aéronautique.

Au-delà de la nature de la couverture, les courtiers ont fait des propositions concernant les *triggers* au cœur de la garantie pour le scénario – est-ce qu'un des triggers – déclencheurs de la couverture c'est l'évènement cyber avec

[14] Chiffres FFA.

une notion de malveillance appréhendée de façon suffisamment large pour ne pas être remise en cause et étendue à l'accidentel en option, le potentiel de remise en cause de la certification aéronautique consécutive à un évènement cyber ou le retrait d'autorisation d'activité par une autorité administrative. Le comité courtier propose également la prise en compte des acteurs de la chaine d'approvisionnement en amont et en aval pour garantir la résilience de l'ensemble. L'objectif étant de garantir les pertes suivantes : la marge brute, le coût du stockage temporaire, les dépenses liées au maintien de l'activité, les frais supplémentaires d'exploitation et la gestion de la crise.

L'hypothèse de départ des assureurs dans leur analyse du scénario était de dire que 100 % des sous-traitants avaient souscrit une assurance. Or, la pénétration actuelle du marché de l'assurance cyber est très faible pour les PMI, ETI et PME. Les couvertures cyber ou classiques ne représentent qu'une partie du risque économique. Il est donc, pour les donneurs d'ordre, essentiel de pouvoir insister sur la mise en place de standards de cyber sécurité partagés et applicables de manière sectorielles, adoptés par la filière et reconnus par différents acteurs ainsi que le respect des clauses de sécurité cyber dans les contrats de sous-traitance – assurés, courtiers, assureurs et réassureurs. En regard, le marché de l'assurance sera attentif à la démonstration de la qualité du contrôle effectif du donneur d'ordre.

Nous recommandons le développement de couvertures d'assurance qui reconnaitront l'effort de connaissance en interne du niveau d'exposition au risque cyber, des investissements en cyber sécurité en regard de standards reconnus et partagé, des efforts de gouvernance en interne mis en place démontrant un niveau de maturité cyber et une capacité à gérer le risque.

Les donneurs d'ordre devraient développer une communication vers le marché pour présenter ces standards sectoriels de sécurité, qu'ils soient compris et reconnus par le marché pour développer, au bénéfice des sous-traitants, des offres d'assurance qui soient attachées aux standards de sécurité et adaptées aux besoins de la filière.

IV. Recommandations consolidées

Recommandations du comité réassurance

Recommandation 1. Définir l'évènement cyber afin que les clauses de contrat d'assurance soient robustes et reconnues par toutes les parties prenantes dans le but de développer la clarté et la robustesse des contrats notamment sur les clauses pertinentes.

Recommandation 2. Poursuivre l'exercice de clarification des polices standards (dommage, RC) pour identifier et réduire les expositions silencieuses ou non affirmatives.

Recommandation 3. Améliorer les outils et méthodes de calcul de cumul et de suivi des expositions en lien avec la clarification des polices et la tarification des clauses cyber dans les contrats standards.

Recommandation 4. Poursuivre la formation, l'information, l'investissement, la prise de conscience de tous les acteurs face au risque cyber et son caractère systémique.

Recommandation 5. Un travail de réflexion doit être poursuivi afin d'étudier et de quantifier financièrement le risque juridique induit par la chaine des responsabilités en matière de recours en responsabilité civile : les recours possibles entre des fournisseurs entre eux en cas de non-respect d'une obligation de moyen de sécurité.

Recommandations du comité courtier

Recommandation 6. Le développement d'outils de profilage du risque cyber appréciant le niveau de maturité en cyber sécurité de l'assuré : prenant en compte la qualité du risque cyber des assurés d'un point de vue technique, de gouvernance avec les éléments financiers nécessaires

Recommandation de l'assuré

Recommandation 7. Le développement de standards de cyber sécurité industriels sectoriels reconnus et partagés par le marché de l'assurance.

Recommandation 8. Le développement de couvertures d'assurance qui reconnaitront l'effort de connaissance en interne du niveau d'exposition au risque cyber, des investissements en cyber sécurité en regard de standards reconnus et partagés, des efforts de gouvernance en interne mis en place démontrant un niveau de maturité cyber et une capacité à gérer le risque

V. Le scénario

Il a fallu itérer la démarche de définition du scénario. Un premier scénario a été écarté car il a été estimé trop catastrophique (ce que certains dénomment un cyber cataclysme). Le scénario 1 mettait en évidence les impacts d'une attaque cyber via la chaine d'approvisionnement mais il ne permettait pas d'atteindre la cible de la recherche : mettre en évidence un impact cyber sur la chaine d'approvisionnement. Les impacts affectaient le *Prime* et éventuellement des fournisseurs de rang 1 mais ne descendaient pas en dessous de la chaine de valeur. Le seul impact pour la chaine d'approvisionnement était l'impact trésorerie. Il n'atteignait pas les objectifs de recherche en termes de richesse et d'analyse pour le monde de l'assurance puisque les conséquences étaient principalement envisagées sur l'intégrateur final et peu portaient sur la responsabilité civile et le dommage.

A l'inverse, dans un second scénario tous les sous-traitants sont affectés par un malware de type NotPetya[15] ce qui permettait de focaliser sur les impacts subis par les fournisseurs qui étaient directement touchés et subissaient soit un arrêt de production soit une baisse de performance.

Dans ce scénario 2 - Skyfleet, les impacts sont chiffrables à 30 jours d'arrêt de la production en termes de perte de chiffre d'affaire (CA) et de pénalités de retard. Les pénalités de retards de l'intégrateur final pouvant être rebasculées sur les sous-traitants à l'origine de ce retard.

L'exercice de recherche a pu se développer avec les courtiers. Ces derniers ont pu être interrogés sur le fait de savoir si les polices tous risques pouvaient couvrir les pénalités, la perte de CA et la reconstitution du système d'information. Charge aux assureurs de répondre ensuite. Un tel exercice permettait d'identifier un chiffre en termes de cumul de portefeuille assurantiel sur l'ensemble de la chaine de sous-traitance mettant en exergue une idée de la gestion du cumul du portefeuille sur un seul évènement du point de vue de la réassurance.

Une option de scénario plus offensive a été envisagée. Elle aurait intégré un malware chez un sous-traitant par un acteur malveillant souhaitant contaminer toute la chaine. Ce malware aurait chiffré des données de répertoire de manière intermittente sur 12h, se mettre en sommeil pendant 3 mois et réapparaître et désorganiser la chaine. Cette option aurait été compliquée à quantifier financièrement et elle n'aurait pas permis de chiffrer le cumul de portefeuille sur l'ensemble de la sous-traitance.

Le scénario 2 – Skyfleet retient donc la possibilité d'une attaque sur le SAP – *System Application and Product for data processing*[16] utilisé en propre pour les gros sous-traitants, ou par les plus petits sous-traitants. Le scénario 2 prend ainsi en compte une vulnérabilité SAP exploitée par un acteur malveillant pour désorganiser la filière en chiffrant les bases de données pour en empêcher l'usage. Modifier des données à l'intérieur du SAP n'est pas simple pour un attaquant mais chiffrer les bases pour faire en sorte qu'elles ne soient plus disponibles est faisable. Les SAP sont certes déployés en modules indépendants mais l'obtention d'un accès administrateur peut offrir une grande liberté de manœuvre à l'attaquant. Un accès SAP au système doit être donné au support. Si c'est ce point qui est attaqué avec des privilèges élevés via une faille

[15] Philippe Wolf, *Pièges et obscurité numérique*, https://www.u-cergy.fr/fr/laboratoires/agora/cahiers-d-agora/numero-2/introduction-1-1-1-4.html

[16] Le SAP est un progiciel de gestion intégrée. Il est un ERP – *Entreprise Ressource Planning* ou un PGI en français – un Progiciel de gestion intégrée. Le SAP permet de lier les différentes fonctions de l'entreprise (comptabilité, finance, production, approvisionnement, marketing, ressources humaines, qualité, maintenance) entre elles grâce à un système d'information centralisé avec un client et un serveur.

logicielle ou via une faille des variantes du logiciel, l'attaque est réaliste. La restauration des SAP des sous-traitants dans la perspective d'une filière qui se doit d'être synchronisée est complexe.

Le choix de l'attaque s'est porté sur une « *not targeted attack* » ce qui permettait d'éviter l'exclusion « *targeted attack* » à laquelle certains assureurs réfléchissent.

À première vue, le scénario 2 n'est pas spécifique à la filière aéronautique comme l'était le premier mais il est réaliste compte tenu de l'actualité de la menace cyber.

Il permet de faire passer le message auprès de la sous-traitance sur l'intérêt d'élever le niveau de cyber sécurité et de souscrire une assurance cyber.

L'occurrence n'est donc pas spécifique au secteur industriel dans le scénario 2 mais les conséquences peuvent l'être au vu de l'impératif de traçabilité – le refus par l'intégrateur des pièces dont la traçabilité n'est pas certaine. La spécificité de la filière aéronautique est, en effet, la certification des processus et des produits. Du point de vue de la logistique, un des éléments le plus perturbateur pour la filière pourrait être la perte de traçabilité de la qualité (dont les éléments sont inscrits dans le SAP), la filière aéronautique étant structurée pour garantir une qualité.

Ce scénario peut également être décliné dans d'autres secteurs industriels comme l'automobile ou la pharmacie.

Un troisième scénario avec une combinatoire de menaces a été écarté car il n'aurait pas permis à la réassurance, dans le cadre de l'exercice, de prendre en charge plusieurs évènements.

V.1. Scénario Skyfleet – l'attaque DOBYCHA

La première étape a constitué en la construction d'un scénario réaliste à la fois techniquement (aspects qualitatifs), financièrement (éléments quantitatifs) et du point de vue de l'organisation de la filière (autour de la plateforme de services sécurisés *BoostAerospace*).

L'annexe 2 (bibliographie) recense d'autres exercices de ce type. Ce scénario n'a pas de prétention prédictive mais l'ambition d'entraîner l'ensemble des acteurs à une meilleure prise en compte du risque cyber et de les préparer à des remédiations efficaces.

L'attaque décrite ci-dessous et intitulée DOBYCHA[17] est le résultat d'une réflexion partagée, grâce à une méthode d'idéation collective, par les membres du groupe de travail, impliqués par la filière aéronautique.

On trouvera, en annexe 7, une rédaction complète du scénario avec ses variantes. Une brève du scénario pourrait être :

Le 1 novembre 2018, les ERP SAP de plusieurs fournisseurs du secteur aéronautique européen cessent brutalement de fonctionner avec des messages d'erreur en relation avec une incapacité à trouver les clés de chiffrement permettant d'accéder aux données stockées.

Le 5 novembre 2018, un message est envoyé à un certain nombre de ces entreprises (touchée, ou non) leur soumettant une demande de rançon (250K€) pour la libération de leurs données.

Plusieurs entreprises tenteront de payer la rançon sans succès.

[17] Aujourd'hui, comme pour les cyclones, on a pris l'habitude de désigner les grandes familles de logiciels malveillants par un nom choisi souvent par les éditeurs des pseudo-vaccins. Cela donne lieu parfois à quelques batailles commerciales souterraines.

Figure 2 – Médiatisation de l'attaque (échantillon)

V.2. Typologie des entreprises touchées

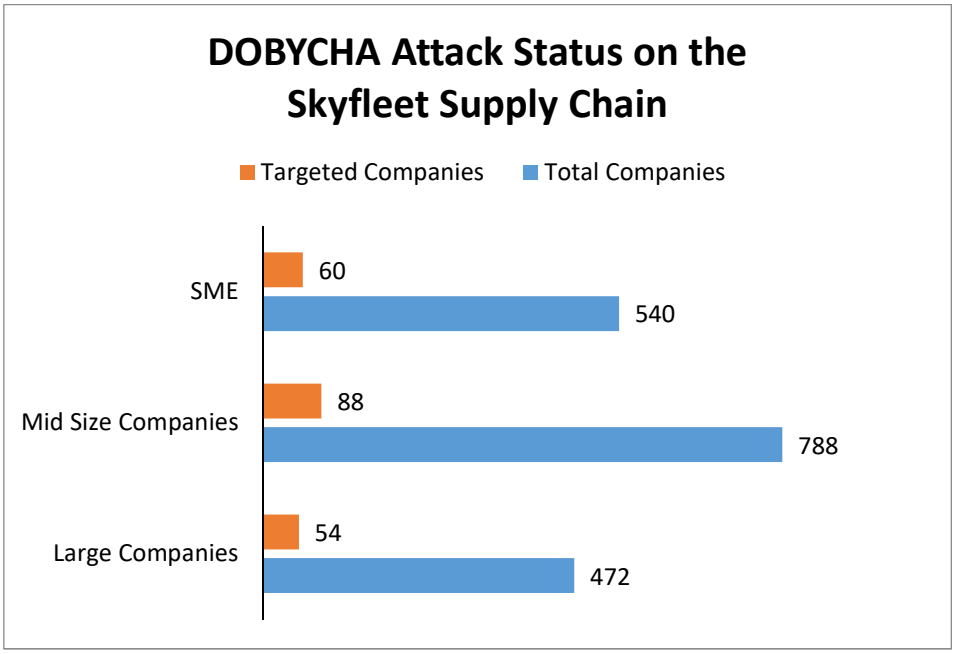


Figure 3 – Entreprises touchées

Les entreprises touchées par l'attaque sont de trois types :

- Type A : 60% réussissent à relancer leur ERP sous 1 semaine (restauration au samedi précédent dans la plupart des cas).

- Type B : 20% restaurent leur ERP à - 1 mois, perdant les informations de configuration de production sur la période manquante. Toutefois certaines informations papiers restent disponibles.
- Type C : 20% ne parviennent pas à restaurer leur ERP et perdent de ce fait l'ensemble des informations de configuration de production à compter du 1er novembre. Seule la réinstallation de zéro du système est possible. Toutefois certaines informations papiers restent disponibles.

V.3. DOBYCHA – le contexte de l'attaque

Le secteur aéronautique européen est porté par le constructeur Skyfleet, et son modèle phare le Skyfleet S410. La flotte de ce modèle se compose de 2 560 avions moyen-courrier en service dans le monde. 1000 avions sont en commande de par le monde à cette date. À titre indicatif et pour les besoins de l'exercice, le prix moyen d'un Skyfleet S410 est de 100M€.

La production des avions est directement impactée à partir du mois de décembre 2018 se traduisant par une baisse des cadences de l'ordre de 10% sur 3 mois. Ce qui représente une impossibilité à livrer une vingtaine d'avion sur la période.

Après 1 semaine d'investigation, les intrusions dans les ERPs ayant conduit à la mise en place de l'attaque peuvent être imputées à un défaut de configuration de ceux-ci lors de leur installation et exploitation.

Une grande majorité des entreprises touchées avaient externalisé l'installation et l'exploitation de leur ERP à la société SG3 (1 des 10 plus grosses ESN européennes).

V.4. DOBYCHA – les détails de l'attaque

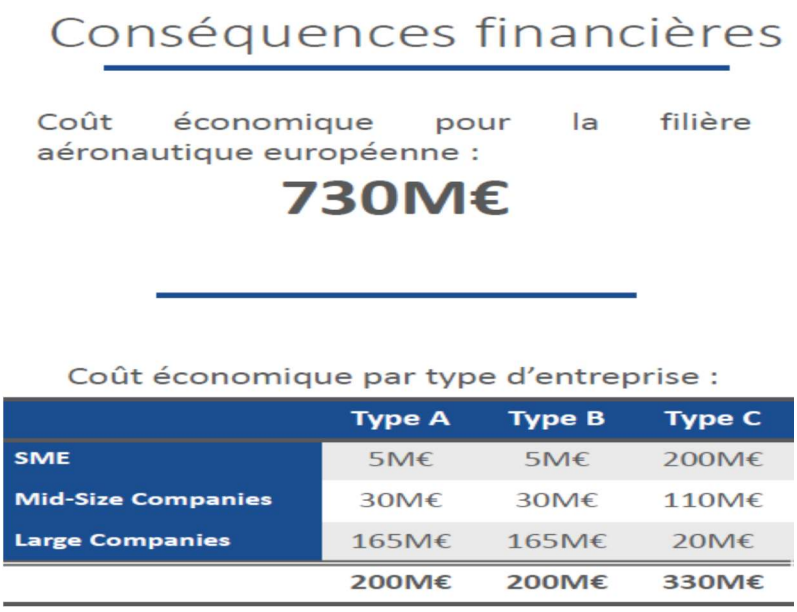
L'attaquant utilise une faille de configuration (couple user/mot de passe faible commun à tous les systèmes impactés) afin d'accéder via un accès distant de maintenance.

En utilisant cet accès, il active une fonction native du système permettant de chiffrer les données de celui-ci (Cette fonction est utilisée habituellement afin d'interdire l'accès aux données de production par un administrateur).

La mise en place de l'attaque prend 1 mois, le temps d'analyser la cible puis de chiffrer les données.

V.5. Conséquences financières

Le coût économique estimé pour la filière aéronautique européenne est de 730M€ répartis selon le schéma suivant.



	Type A	Type B	Type C
SME	5M€	5M€	200M€
Mid-Size Companies	30M€	30M€	110M€
Large Companies	165M€	165M€	20M€
	200M€	**200M€**	**330M€**

Figure 4 – Coûts économiques par type d'entreprise. (synthèse)

VI. Réponse des courtiers

Les premiers travaux en comité ont réuni les courtiers lesquels se sont attachés à voir comment le scénario pouvait être compris et transcrit dans un langage compréhensible par leurs clients et les assureurs. Une réflexion a été engagée sur la situation hétérogène des acteurs de la filière. Les TPE PME n'ayant pas besoin des mêmes capitaux que les grands acteurs mais néanmoins le besoin d'un même niveau de garantie. Une seconde réflexion a porté sur le design du programme pour gérer l'hétérogénéité des acteurs, quel serait le cahier des charges à écrire pour obtenir de l'assurance la meilleure couverture pour la filière.

Membres du Comité Courtiers d'Assurance

- Guillaume Deschamps (GRAS SAVOYE) ;
- Nicolas Hélénon (NEOTECH - LSN) ;
- Mickaël Robart (SIACI SAINT HONORE) ;
- Jean-Laurent Santoni (Clever Courtage) ;
- Luc Vignancour (MARSH).

Philippe Wolf (IRT) et Bénédicte Suzan (Airbus).

VI.1. Préalable

Les membres du Comité Courtiers d'Assurance ont souhaité placer leur réflexion dans un contexte global qui dépasse celui du cas pratique soumis à leur analyse afin de l'inscrire dans les différentes filières dépendantes de leur *supply chain* et soumises à des obligations de certification. En effet, comme d'autres filières (industrielles, pharmaceutiques, agro-alimentaires, …) la spécificité de la filière aéronautique tient à la certification au PAO et à son organisation autour de la plateforme d'échange entre les fournisseurs BoostAeroSpace (par abréviation BAS) dont les membres fondateurs sont Dassault, Safran, Thales et Airbus.

Il a donc été postulé que le scénario Skyfleet était à contextualiser autour des entreprises membres de *BoostAerospace* qui met en place dans le cadre du projet AirCyber des standards de cyber sécurité pour lesquels les membres fondateurs souhaitent que les sous-traitants investissent pour élever leur niveau de maturité. *BoostAerospace* étudie des options de *business model* incluant le financement du risque cyber par le transfert du risque résiduel à l'assurance. Une interrogation porte également sur l'inclusion dans les contrats d'achat des acteurs de rang 1, des clauses d'assurance cyber. Le financement du risque pourrait constituer un retour sur investissement en cyber sécurité. Enfin, un point important en matière de recours et de responsabilité civile réside dans la question de savoir si les membres fondateurs de la plateforme sont tiers entre eux.

Pour des raisons industrielles de production, il a été trouvé opportun d'approuver, en premier, la définition d'un produit (aéronef, hélice, moteur) puis d'émettre des certificats de navigabilité individuels aux produits (aéronefs) après démonstration de leur conformité à la définition.

La certification d'un aéronef (le processus de certification ne concerne pas seulement les aéronefs mais aussi les moteurs et les hélices) est le processus par lequel l'autorité de conception délivre, à un industriel concepteur d'un aéronef, un ***Certificat de Type*** et qui atteste que l'aéronef, définit par sa ***Définition de Type***, répond en tout point aux exigences techniques de navigabilité applicables. Le Certificat de Type est accompagné de la fiche de navigabilité (TCDS : *Type Certificate Data Sheet*) qui définit le produit et ses caractéristiques (nomenclature, limitations…). Ensuite, l'aéronef est produit en conformité avec la définition

de type préalablement approuvée par l'autorité de conception. Deux organismes interviennent le plus souvent dans la conception et la fabrication d'un aéronef ou d'un produit :

- DOA (*Design Organization Approval*) : Organisme approuvé par l'autorité compétente suivant des exigences réglementaires pour concevoir un produit (aéronef, hélice, moteur). L'organisme doit démontrer et vérifier la conformité du produit aux règlements de navigabilité et il doit déclarer et justifier à l'autorité de conception cette conformité ;
- POA (*Product Organization Approval*) : Organisme approuvé par l'autorité compétente pour fabriquer un produit en conformité avec sa définition de type approuvée.

Figure 5 – Certification d'un aéronef

La spécificité de la filière aéronautique réside donc dans la certification de la chaine de production[18] en amont de la certification de l'avion en vol. L'intégrateur final et tous les sous-traitants doivent être en mesure de prouver que tout ce qui a été produit l'a été conformément au cahier des charges du design de l'avion, conformément à la configuration prévue par le bureau d'étude. L'avion doit être certifié conforme à ses spécifications. Pour pouvoir garantir une production conforme à la configuration, il est important pour chaque entreprise sur la chaine de la valeur de la conserver. Avec la digitalisation des *process* de fabrication, la majorité des éléments de configuration qui permettent de prouver la maitrise de la fabrication se trouve dans l'ERP. Conserver les données sous format papier fait partie des procédures en place. Si les procédures de back up ont correctement été mises en place, les moyens de prouver la conformité de ce qui a été déjà produit existent. Mais si le fournisseur n'est pas capable de remettre son ERP en fonctionnement nominal, la certification tombe et le *process* pour la récupérer prend du temps, plusieurs mois voire un an

[18] Cette certification délivrée par l'EASA (European Aviation Safety Agency) s'appelle un POA Production Organisations Approval. Voir ce lien : https://www.easa.europa.eu/easa-and-you/aircraft-products/production-organisations-approvals et l'annexe 1. Son équivalent américain est émis par la FAA Federal Aviation Administration voir https://www.faa.gov/aircraft/air_cert/production_approvals/prod_cert/pc_regs/

potentiellement. L'enjeu ne sera pas de remettre en fonctionnement l'informatique mais de garantir le maintien de la certification.

La garantie d'assurance doit également pouvoir être activée pour les fournisseurs qui sont en mode SaaS. Se pose la question de la problématique de cumul chez le prestataire qui délivre des prestations en mode SaaS aux fournisseurs de la chaine d'approvisionnement d'Airbus. Se pose également la question de la nécessité d'une politique de sécurité en place et contrôlée.

VI.2. L'analyse opérée par les membres du Comité Courtier

Globalement il s'agit de prendre en considération que ce qui vaut pour cet écosystème de l'aéronautique vaut également pour d'autres secteurs industriels comme par exemple pour le secteur pharmaceutique ou l'automobile. Les réflexions menées dans le cadre de ce séminaire peuvent être appliquées à d'autres domaines.

Pour rendre cette problématique assurable, il faut l'encadrer, l'encapsuler dans un écosystème. *BoostAerospace* est intéressant car il permet d'adosser l'assurance ou l'assurabilité à une évaluation de la maturité en cyber sécurité de l'ensemble de ses acteurs. Dans une chaine aéronautique, les différents fournisseurs de différents rangs, participent tous à l'intégration d'un ensemble d'éléments fournis par l'ensemble des acteurs. Cet assemblage est gouverné de bout en bout – la certification du droit à produire conformément au design du bureau d'étude pour délivrer un produit qui soit conforme aux éléments d'assemblage.

L'originalité et la complexité du montage d'assurance est la concomitance ou le couplage d'un évènement cyber et d'une perte de certification. Les discussions du comité courtier ont insisté sur les triggers – qu'est ce qui déclenche la garantie. L'est-elle par l'évènement cyber, par la perte de certification, par les deux, en amont, en aval ? Si on veut mettre en place un dispositif d'assurance qui ait une pérennité et un équilibre, une économie du contrat pour permettre aux assureurs et aux réassureurs de répondre à leurs obligations du pilier II de Solvency – comprendre le risque de provisionner, de déterminer la prime et d'équilibrer en cas de sinistre – l'accompagnement en cas de crise est extrêmement important. Le vrai sujet est l'approche de la garantie ne peut s'inscrire qu'en financement adossé au *Procurement* – à l'ensemble des contrôles d'achat et de maturité des différents acteurs.

En conséquence la présentation à l'assureur n'est pas un questionnaire technique sécurité informatique tel que découlant par exemple de l'ISO 27000. La complexité technique va évoluer. Du point de vue de l'assurance, la question est : qu'est-ce qui déclenche la garantie et qu'est-ce qu'on paye en cas de sinistre ? Corrélativement, en fonction de cette probabilité et de cette quantification de l'évènement, quel niveau de garantie est nécessaire et quel est le niveau de prime qui permet d'équilibrer le risque.

La problématique a été découpée en plusieurs aspects : la souscription – vraie question entre un questionnaire technique, un profilage et une analyse car la chaine d'approvisionnement comprend les intégrateurs finaux, des moyennes et des petites entreprises pour lesquelles la problématique est tout aussi importante. On va également retrouver la problématique selon laquelle tous les fournisseurs ne fournissent pas que la chaine aéronautique. Si un évènement sur l'ERP survient, est-ce que le contrat va prendre en compte l'indisponibilité de leur système d'information dans leur capacité à produire ? Est-ce que l'indemnisation va porter sur la totalité de l'indisponibilité ou la seule part de chiffre d'affaire dédiée à la chaine d'approvisionnement de l'aéronautique ? Si un fournisseur fait 10% de son chiffre d'affaire avec Skyfleet pour reprendre le cas pratique, est-ce les 90% sont couverts ? Un GPS peut être mis dans un avion, une voiture, un navire. En cas d'interruption quel est la part de son chiffre d'affaire qu'il va privilégier,

comment sera-t-il indemnisé ? Ce GPS peut également être intégré dans la chaine de valeur d'un autre avionneur – les règles de conformité sont les mêmes ou proches pour les avionneurs selon l'EASA (*European Aviation Safety Agency*) et la FAA (*Federal Aviation Administration*).

Le questionnaire n'est pas tant un questionnaire de risque mais de profil et d'analyse de maturité.

Sur le design du programme, la question est qu'est-ce qui déclenche la garantie ? On peut avoir un évènement informatique pour ceux qui ont l'ERP et avoir du fait de cet évènement une perte de certification et le co-contractant ou un fournisseur du rang du dessus n'a peut-être pas le même problème cyber mais s'il ne reçoit plus de pièce certifiée il ne peut plus produire – son trigger n'est donc plus un problème de cyber mais de perte de certification. Comment cela est-il constaté et prouvé ?

Autre considération, l'ERP a été fourni par un fournisseur de logiciel et il faut articuler le recours de l'assureur et éventuellement sur la RC pro du fournisseur du logiciel pour savoir si ce logiciel répond aux règles de « *security by default* », conforme et s'il y a éventuellement un recours.

Dans le montage des contrats d'assurance, on comprend bien leur caractère collectif puisqu'il protège un ensemble de population qui est hétérogène et dont 100% du CA ne sont pas dédiés à la chaine aéronautique. En outre, le scénario propose des complexités croisées.

VI.2.a. Question préalable : quel est le niveau de couverture d'assurance actuel au regard du scénario retenu pour l'étude ?

En préalable la question a été soulevée de savoir quel serait le niveau de couverture au moins des 1.800 entreprises fédérées autour de *BoostAerospace*, si le scénario retenu se réalisait aujourd'hui[19].

En assurance de dommages, à défaut de souscrire une police d'assurance spécifique cyber, c'est-à-dire couvrant une atteinte immatérielle malveillante aux systèmes et aux données, il est à craindre que les polices d'assurances traditionnelles Tous Risques Informatiques couvrant un évènement matériel ne puissent couvrir le scénario redouté. La couverture qui résulterait de la mise en cause des prestataires externes (ERP en mode SaaS) se heurterait aux stipulations contractuelles et à la démonstration d'une faute éventuelle de l'éditeur (*security by default*). La perte de certification consécutive à un évènement cyber parait également non prise en compte dans les contrats classiques, a fortiori si cette perte de certification touche un acteur de la chaine d'approvisionnement qui n'aurait pas subi directement l'atteinte cyber. Le retrait d'autorisation d'activité par une autorité administrative, soit la suspension temporaire supposera d'examiner le fait générateur qui a donné lieu à cette mesure et il est probable que la mesure fondée sur un risque potentiel ou la mesure de précaution pour éviter sa propagation ne soit pas expressément visé dans le contrat. Au titre des frais et pertes, frais de gestion de crise et pertes d'exploitation, le déclenchement de leurs prises en charge supposera que le fait générateur initial soit spécifiquement défini comme résultant d'une atteinte cyber.

En assurance de responsabilité, le fondement classique de la garantie « *claims made* » supposera la réclamation d'un acteur de la chaine d'approvisionnement dirigé selon les circonstances en amont ou en aval, mais dans un contexte d'interdépendance, à examiner au regard des stipulations contractuelles

[19] On lira avec intérêt le retour d'expérience fait à l'occasion des rencontres annuelles des *risk managers* du 7 au 9 février 2018 par Claude Imauven, directeur opérationnel du groupe Saint Gobain, chiffrant à 220 millions d'euros de chiffre d'affaires la perte subie par son Groupe lors de l'attaque cyber NotPetya en juin 2017. Lire https://www.usinenouvelle.com/editorial/chez-saint-gobain-il-y-un-avant-et-un-apres-la-cyber-attaque.N651134

(limitation contractuelle, considération de la qualification de force majeure ou pas de la décision de retrait d'autorisation de produire ou de la suspension imposée par une autorité administrative type ANSSI, ...).

Si les polices de responsabilité classique couvrent la responsabilité d'un produit aéronautique défectueux, il sera difficile de l'appliquer à un produit non fabriqué, ou fabriqué sans traçabilité. Si l'on considère que les membres de la chaine d'approvisionnement ne sont pas nécessairement liés entre eux par un contrat, la mise en œuvre d'une responsabilité extracontractuelle risque de faire surgir des problématiques de *silent cover* importantes. La question du recours à l'encontre de l'éditeur de l'ERP risque également de donner lieu à un contentieux judiciaire au résultat incertain et à la mise en œuvre qui peut s'avérer très longue dans le temps comme on l'a vu plus haut.

La conclusion est apparue rapidement que, en l'état et à de quelques rares exceptions liées à la souscription de contrats cyber souvent orientés vers la couverture des atteintes aux données personnelles et au financement des coûts de notification *privacy*, le scénario retenu n'était pas actuellement couvert dans les programmes d'assurance des acteurs de la chaine d'approvisionnement.

VI.2.b. La problématique de souscription

- **Le Questionnaire de *BoostAerospace*, une première base**

La certification et *BoostAerospace* permet d'établir un rating des sociétés avec un niveau requis de maturité du risque cyber et du risque digital de manière générale. Ces deux filtres sont considérés comme étant sécurisant. Au regard du questionnaire de *BoostAerospace*, la question d'assurance n'est pas de démontrer un niveau en cyber sécurité. Le questionnaire est en effet assez précis sur la gouvernance y compris sur des questions techniques portant sur la résilience des acteurs. Ce questionnaire conduit à l'acquisition des standards *Gold*, *Silver*, *Bronze*. Un audit est conduit annuellement pour s'assurer que le fournisseur répond aux engagements de sécurité des labels. Conformément à l'ISO 27000, la politique de sécurité est réévaluée tous les ans.

D'un point de vue *Risk Assesment* de la résilience de l'entreprise et sa gouvernance du risque, ce filtre peut suffire et fonctionner pour l'assurance comme un pré requis.

Le questionnaire de *BoostAerospace* est adaptable à tous les fournisseurs de la chaine d'approvisionnement de l'aéronautique quel que soit le donneur d'ordre. Il adresse la résilience au risque cyber et la résilience en terme technologique, d'organisation et de continuité dans la perspective, pour le fournisseur, d'être en mesure de livrer des éléments certifiés. Il y a une forte liaison entre le risque du donneur d'ordre de se trouver confronté à l'indisponibilité de fourniture ou à la fourniture d'une pièce non conforme. L'indisponibilité pouvant être la conséquence d'un évènement cyber – cet évènement pouvant être partagé par l'ensemble des acteurs. Le risque d'un ERP partagé est à la fois concentré sur l'indisponibilité du système. C'est un risque supplémentaire sur le fait que l'indisponibilité du système par les uns peut entraîner la perte de conformité de la production d'un élément. Ce risque va s'agréger à celui d'un autre fournisseur mis dans l'incapacité de fournir en amont ou en aval.

- **… à développer pour orienter le questionnaire pour le marché de l'assurance**

La connaissance par le marché de l'assurance porte davantage sur le risque financier encouru par les sous-traitants et sur leur capacité à soutenir le risque, étant entendu qu'une grande partie de ces entreprises sont de taille moyenne voire de petite taille. Leur structure financière ne leur permettrait de résister que quelques semaines – 15 jours, 3 semaines… Or si le trigger retenu est la perte de certification, cela pourra

prendre plusieurs mois voire une année pour être autorisé à participer de nouveau à la chaine d'approvisionnement.

L'idée est de s'interroger sur le risque de dépendance des acteurs de la chaine d'approvisionnement de l'aéronautique en fonction du % du CA et sur la structure financière de l'organisation – comment la trésorerie supportera effectivement une problématique d'arrêt de l'activité et de vente. Ces calculs se font facilement et les informations sont récupérables quel que soit l'évènement (incendie, dégât des eaux). Le questionnaire cherchera donc à définir l'interopérabilité et la dépendance aval et amont de ces acteurs car on peut imaginer qu'un acteur n'ayant pas subi directement l'évènement ne puisse pas intégrer la chaine de valeur. Les PCA des donneurs d'ordre imposent à la chaine d'approvisionnement des modalités de résilience (ralentissement de la production, stockage…) mais au-delà de plusieurs semaines ou mois, la production doit s'arrêter. La difficulté s'accroît si, consécutivement à l'évènement cyber, la certification tombe. Elle peut ne pas être concomitante à l'évènement cyber. La dimension temps est importante. Le questionnaire devra traiter l'interaction entre les acteurs, la surface financière et la capacité à survivre après de tels évènements.

L'objectif est double. Apporter le maximum d'information aux assureurs sur l'appréciation des risques qu'ils seraient amenés à couvrir, ces informations de souscription ayant également pour objectif d'obtenir le support d'un maximum de souscripteurs. Et pour les sociétés qui rejoindront le schéma et souhaiteront s'assurer contre les conséquences financières d'incident cyber qui pourraient les concerner directement ou par ricochet, le but est de leur permettre de bénéficier de garanties qui prendront en considération la maturité de leur gestion du risque cyber afin de différencier les risques acceptables ou pas.

Le profil de risque et la taille des entreprises sont deux éléments à prendre en considération. Certains questionnaires peuvent être compliqués à remplir et peuvent dans certains cas conduire à stopper les discussions. Comment aborder le processus de façon simple tout en apportant aux souscripteurs et assureurs, les informations nécessaires pour accompagner correctement cette démarche ?

La prochaine étape pour les courtiers est d'élaborer sur la base d'informations existantes – les labels *Gold*, *Silver* et *Bronze* et de les compléter par l'élaboration d'un questionnaire simple élaboré par ce que les courtiers voient aujourd'hui sur le marché en faisant en sorte de se limiter sur les questions principales qui permettront aux assureurs de prendre position sur la souscription du risque. Sur la base d'un document qui présenterait le contexte général de l'environnement dans lequel ces sociétés évoluent.

Le questionnaire courtier permettra de connaître les échelles de grandeur, d'aborder la réflexion sur le risque systémique – l'interdépendance des acteurs et d'apporter des éléments sur l'agrégation des pertes potentielles maximum possibles.

Dans le scénario proposé, il faudrait connaître la part du CA du fournisseur imputable à Skyfleet ainsi que la ventilation du CA des fournisseurs en relation contractuelle pour calibrer les niveaux de garantie, unitairement et en cumul ainsi que les délais, les SLA et les pénalités contractuelles.

Cette manière de faire permet également de maintenir les obligations de déclaration du risque à l'assureur imposées par le Code des assurances, le questionnaire signé servant de déclaration du risque par chaque fournisseur à la souscription.

VI.2.c. Le design du programme d'assurance

- **Les triggers de la garantie et le contenu du contrat**

La présentation des informations au marché de l'assurance porte d'abord sur un socle commun : permettre la résilience de la filière. L'objectif de l'exercice n'étant pas de permettre au donneur d'ordre final de se faire

indemniser d'une défaillance d'un des acteurs de la chaine d'approvisionnement mais de permettre aux entreprises de survivre et de maintenir leur activité.

L'exercice s'inscrit dans le contexte de la filière et de l'interdépendance des acteurs. Le socle commun prend en considération le dommage, le first party moins la RC pour éviter la problématique de la mise en cause des acteurs.

Les triggers au cœur de la garantie :

- L'évènement cyber avec une notion de malveillance appréhendée de façon suffisamment large pour ne pas être remise en cause et étendue à l'accidentel en option. La recommandation est d'écarter la question de l'attribution (i.e. l'acte de malveillance doit être reconnu sans rechercher à qui l'attribuer et quelles sont les motivations).

L'évènement cyber malveillant pourrait être ainsi défini : l'utilisation non autorisée d'un système d'information ou le fait d'empêcher un système d'information de fonctionner.[20]

- La perte de certification consécutive à un évènement cyber.
- Le retrait d'autorisation d'activité par une autorité administrative, soit la suspension temporaire.

Au-delà du cœur de la garantie, prendre en compte les acteurs de la chaine d'approvisionnement en amont et en aval pour garantir la résilience de l'ensemble.

- L'indisponibilité d'un fournisseur et d'un client sur un évènement dénommé et lié à un évènement cyber ou à une perte de certification ou à une injonction d'arrêt d'une autorité.

Il s'agit de retrouver les trois éléments principaux des défaillances du fournisseur ou du client.

L'objectif recherché derrière ces *triggers* est :

- De donner les moyens à l'entreprise de survivre, de continuer à produire et de repartir. Les impacts financiers principaux à prendre en charge sont tout ce qui est la conséquence d'une réduction ou d'un arrêt de la production : perte de marge brute, coûts de stockage, temporaires… tout ce qui va se retrouver dans une garantie de Perte d'exploitation.
- de faciliter et d'accompagner le redémarrage de l'activité, prendre en compte l'ensemble des dépenses qui seront engagées pour maintenir l'activité, travailler autrement, redémarrer, comprendre et investiguer.
- La prise en compte de la partie « gestion de crise » mais qui doit faire l'objet d'un appel d'offre distinct afin que le prestataire réponde aux critères de confiance de la chaine d'approvisionnement du point de vue de la résilience du secteur aéronautique et de défense.

Les pertes à garantir sont :

- la marge brute ;
- le coût de stockage temporaire ;

[20] Pour l'essentiel il s'agit des infractions visées au Code Pénal Chapitre III : Des atteintes aux systèmes de traitement automatisé de données (Loi n° 88-19 du 5 janvier 1988. relative à la fraude informatique dite Loi Godfrain)

- les dépenses liées au maintien de l'activité ;
- les frais supplémentaires d'exploitation ;
- la gestion de crise.

Le but étant de permettre la survie de l'entreprise – soit 15 jours de trésorerie pour les petites, les conséquences du ralentissement de l'activité – la marge brute sont prises en compte ainsi que l'ensemble des dépenses qui doivent être engagées par l'entreprise.

Reste le sujet des pénalités commerciales imposées par les donneurs d'ordre finaux qui devraient rentrer dans les impacts financiers de l'interruption de l'activité. Le sujet est ouvert quant à savoir s'il doit être inscrit dans le programme d'assurance final.

- **La problématique RC et son lien avec la RC Pro**

Concernant les pénalités contractuelles, outre celles vis-à-vis du donneur d'ordre de l'aéronautique, les acteurs de la chaine font face également à celles de leurs autres donneurs d'ordre. Ils font face également à celles des tiers suite à des mises en cause consécutives à des violations de données – RGDP. Les ERP contiennent les données RH et commerciales.

Le Comité Courtier a préconisé de se limiter à l'assurance Dommage pour éviter les mises en cause croisées en responsabilité civile. Mais, le socle commun pourrait être enrichi des garanties complémentaires liées à la RC et la RC pro.

Une vraie question est posée pour le fournisseur de l'ERP qui doit intégrer un niveau de sécurisation. Le questionnaire du *Procurement* n'impose pas tel ou tel modèle d'ERP ou d'architecture de sécurité. Un certain nombre de facteurs de sécurité devait être intégré – mise à jour, *patch management*. Si tel n'est pas le cas, et s'il y a exploitation d'une faille d'ERP, il existe un risque majeur de recours en RC pro contre l'éditeur.

Deux autres acteurs doivent être observés dans leurs responsabilités : celui chargé par l'entreprise d'installer et d'exploiter le logiciel ERP ; ou bien le fournisseur de service ERP en mode SaaS par d'autres acteurs.

Le scénario vise autant les entreprises qui disposent de la solution ERP installée dans leurs locaux ou celles qui l'ont en mode SaaS. Il met en exergue une erreur de la part de l'installateur.

- **Contrat individuel, contrat collectif ou pour compte ? Quelle formalisation ?**

Quel choix entre contrat individuel ou les deux ? Sachant que les entreprises ne vont pas cumuler différentes approches. Il s'agit de réfléchir à quelque chose qui soit facile à souscrire dans ce contexte. Cela pose la question de savoir quelle est l'approche la plus appropriée entre un contrat individuel ou collectif ; voir un contrat pour compte. On peut imaginer qu'un industriel s'assure tant pour ce compte pour qui il appartiendra vis-à-vis de ses différents acteurs.

Les règles du contrat en matière de souscription pour compte : les problématiques de présentation d'assurance pour compte dans ce contexte-là, quelle formalisation du contrat ? Contrat individuel, contrat collectif, contrat individuel avec une première ligne, contrat collectif avec une première ligne, une deuxième ligne … Les besoins de capitaux ne seront pas les mêmes – des petites entreprises fabricant des éléments très importants, des duplications …

La recommandation, pour que cela fonctionne et que la réponse soit efficace, est un texte commun et un pool d'assureur pour que chacun prenne sa part, mais qu'il y ait une part acceptable par chacun (10% ?).

Le sujet individuel et collectif n'est pas indissociable. Il peut y avoir un socle commun et une approche mutualisée collective. La capacité n'est pas indéfinie. On peut imaginer que le risque systémique soit géré par un *stop loss*, par une capacité annuelle maximum pour l'ensemble des acteurs même si chacun des acteurs individuellement souscrirait les garanties qu'il souhaite – le socle plus les garanties complémentaires et les niveaux de garanties qui dépendront des garanties du questionnaire de *BoostAerospace*, ses labels et la prérequis de la certification. Les montants de la garantie souscrite seront ainsi limités en fonction de la qualité du risque. Ces définitions pourront être garanties d'entrée de jeu. Ou bien cela peut être géré par la franchise. 5 ou 6 critères peuvent suffire. De telles approches sont déjà développées par les assureurs dans certains domaines pour des petits risques.

Les notions d'individualisation du risque et de gestion de la mutualisation du risque systémique peuvent être conciliées. Les deux options sont sur la table. Tout dépend de ce qui serait accepté par le marché de l'assurance. Est-ce que le marché de l'assurance est prêt à souscrire un contrat cadre sur la base d'information globale dans un écosystème homogène et quantifié ? Ou bien, le marché préfèrera faire une souscription au cas par cas sur la base d'un questionnaire simplifié pour apprécier au cas par cas chaque risque. Chacune des deux visions a ses avantages et inconvénients.

Quelle est la démarche à suivre pour répondre à notre enjeu ? Faut-il se réunir pour écrire un texte correspondant aux besoins de la filière, aux différents *triggers* pour trouver un accord sur les termes et les déclenchements afin de définir un vocabulaire commun pour des définitions, savoir ce que l'on paye à qui à quoi. Des offres aujourd'hui sur le marché indemnisent avant même que l'évènement ne se produise car il est plus financièrement rationnel de limiter la propagation du risque plutôt que d'attendre. Voir, par exemple, les offres des Lloyds.

En cas d'attaque importante, l'ANSSI pourrait également « demander » ou fortement suggérer aux acteurs de la filière qui ne sont ni OIV ni OSE de couper leurs systèmes d'information pendant une durée à définir – probablement quelques jours le temps de comprendre et de circonscrire l'attaque. Dans ce cas, le trigger pour la majorité de ces sociétés ne serait pas un problème cyber direct mais plutôt la demande d'une autorité administrative. Comment calculer les SMP sur des périodes réalistes (1heure / 1 jour / 1 semaine / 1 mois).

- **Une solution de juste milieu doit être recherchée.**

L'intervention de l'ANSSI pourrait être prévue dans les *triggers* de couverture comme étant un impact collatéral d'une décision prise par une autorité. Du point de vue de l'assurance, les points saillants sont liés au fait que les assurés ne doivent pas être tiers entre eux, les problématiques de recours, qui est souscripteur, comment répartir les primes, comment faire évoluer un contrat opposable aux modifications. La question de l'assurance de l'intangible touche également à la capacité même du marché de l'assurance de répondre aux besoins d'assurabilité des assurés. Est-ce que l'assuré est prêt à financer ce genre de couverture ?

VI.2.d. Prochaines étapes

- **Quel pourrait être un *wording* partagé ?**

Les éléments du *Procurement* permettent une visibilité plus grande qu'y aller en ordre dispersé. Il s'agit d'éviter une souscription protéiforme, non contrôlée, diffuse et peu comprise par les assureurs. En cas de sinistre, il faut un lieu de centralisation de l'information pour obtenir un retour sur expérience pour faire évoluer la connaissance pour la meilleure compréhension d'un risque qui sera systémique. Il s'agit d'éviter

en cas de sinistre une mauvaise réponse du marché, une absence de garanties, ou qu'elles soient au mauvais niveau.

- **Identification du reste à charge pour l'industrie**

NB : en l'état actuel (voir préalable) le reste à charge est total.

VII. Réponse de l'Assurance

Le groupe de travail assurances a mené, à partir de sa compréhension du scénario et des demandes exprimées par les courtiers, une double analyse :

1. Autour des couvertures à proposer à la filière aéronautique, organisées par paquets de garantie.
2. La quantification de cette couverture dans le cadre précis du scénario proposé.

La retranscription intégrale de l'analyse fournit dès lors une méthodologie applicable à d'autres événements cyber. Cette méthode s'affinera sûrement à l'épreuve d'une réalité dont il sera difficile d'anticiper les caractéristiques, très liées à l'ampleur de la transformation numérique dans les entreprises et aux nécessaires progrès de leur résilience (en informatique, capacité d'un système d'information à résister à une panne ou à une cyberattaque et à revenir à son état initial après l'incident).

VII.1. Rappel du scénario

VII.1.a. Timeline

Le 1er novembre 2018, les ERP (logiciel de gestion) de plusieurs fournisseurs du secteur aéronautique européen cessent brutalement de fonctionner.

Leurs utilisateurs sont dans l'incapacité de trouver les clés de chiffrement permettant d'accéder aux données stockées.

Rançongiciel (*Ransomware*) : le 5 novembre 2018, un message est envoyé à un certain nombre de ces entreprises (touchée ou non) leur demandant une rançon pour la libération de leurs données.

Le montant de la rançon est fixé à 250 000 € pour un retour des clés de chiffrement utilisées.

Plusieurs entreprises tenteront de payer la rançon pour se rendre compte que les moyens de communication fournis par l'attaquant sont inopérants.

Trois types d'entreprises sont touchés. Les entreprises A, pour lesquelles il y a peu d'impact : une semaine d'arrêt de production – 60%. Les entreprises B pour lesquelles les impacts sont estimés à 15 jours d'arrêt de production et une remise à niveau progressive sur un mois – et les entreprises C qui subissent 6 mois d'arrêt de production et une perte de l'agrément pour fournir les pièces aéronautiques.

VII.1.b. Descriptif

L'attaquant a utilisé une faille de configuration des ERP afin d'y accéder via un accès distant de maintenance.

En utilisant cet accès, il active une fonction native du système permettant de chiffrer les données de celui-ci.

L'attribution est difficile. Soupçons de motivations géopolitiques et économiques…

Utilisation d'un défaut de configuration des ERP imputé à un défaut d'installation et d'exploitation (l'installation et l'exploitation des ERP sont externalisées à la société SG3).

VII.1.c. Chiffres clés

Les entreprises attaquées travaillent pour le constructeur aéronautique Skyfleet dont le modèle phare est le Skyfleet S410.

La flotte de ce modèle se compose de 2560 avions moyen-courrier en service dans le monde.

1000 avions sont en commande à cette date.

Le prix moyen d'un Skyfleet S410 est de 100M€.

VII.1.d. Résumé

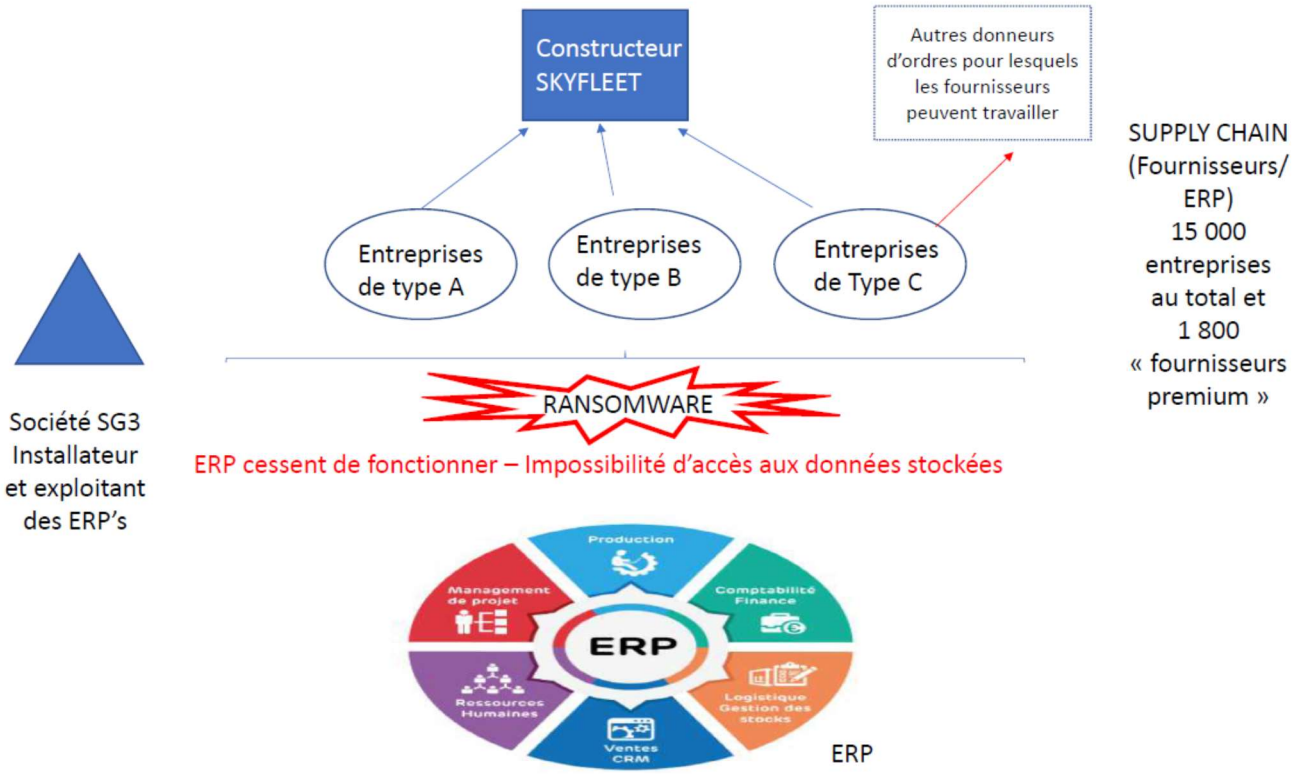


Figure 6– Schéma résumé de l'attaque

VII.2. Autres éléments d'information

***Triggers* identifiés par les courtiers**

- Évènement principal : attaque cyber malveillante
- Perte de certification due à l'évènement Cyber
- Retrait d'autorisation d'activité d'une autorité administrative

NB : Les courtiers ont soulevé la question de la souscription d'un contrat individuel ou d'un contrat de groupe.

Cela pose également la question de l'engagement maximal et de la problématique des contrats franchisés lorsque les sous-traitants sont interconnectés entre eux.

VII.3. Livrables attendus

Rappel des objectifs

- Finalité de l'exercice

- Tester le scénario de risque cyber sur l'ensemble de la chaine de la valeur depuis les fournisseurs jusqu'à l'intégrateur final dans le domaine industriel de l'aéronautique et de la défense.

➢ Quatre objectifs principaux

- Comprendre l'ampleur du scénario du point de vue du *risk manager*, le qualifier et le quantifier financièrement.
- Etudier la réponse du marché de l'assurance cyber (courtiers, assureurs, réassureurs) en termes de couverture du risque pour tous les acteurs de la filière : depuis les ETI jusqu'aux grands groupes.
- Comment les assureurs gèreraient, le cas échéant, la quantification, la souscription et l'accumulation ?
- Identifier les domaines assurables et non assurables qui laissent à la charge de la filière des risques non assurables résiduels pour lesquels elle doit s'organiser.

VII.4. Approche cyber du scénario

VII.4.a. Les fournisseurs

Quels dommages ?

En fonction des catégories d'entreprises victimes :

1) **Les entreprises qui réussissent à relancer leur ERP sous 1 semaine** : 60 % du total (Entreprise de type A)

➢ Conséquences dommageables :

- a) 1 semaine d'arrêt de production sans autres conséquences

2) **Les entreprises qui réussissent à relancer leur ERP sous 1 mois** : 20% du total (Entreprise de type B)

➢ Conséquences dommageables :

- a) 15 jours d'arrêt de production, puis 20% de baisse de rendement de production pendant 1 mois
- b) Perte de toutes les données gérées par l'ERP (les informations de configuration de production) et notamment de production sur la période manquante, toutefois certaines informations papiers restent disponibles
- c) Remise en question du POA (Production Organisation Approval) par l'AESA (Agence Européenne de Sécurité Aérienne) impliquant un surcoût de production de 10%

3) **Les entreprises qui ne réussissent pas à relancer leur ERP :** 20% du total (Entreprise de type C)

➢ Conséquences dommageables:

- a) Retour à la capacité de production sous 6 mois
- b) Perte de toutes les données gérées par l'ERP (les informations de configuration de production) et notamment de production à compter du 1er novembre. Toutefois certaines informations papiers restent disponibles
- c) Obligation de reconfigurer entièrement le système

- d) Perte du POA

Autres conséquences dommageables pour l'ensemble des entreprises fournisseurs (A, B et C)

- Pénalités contractuelles ;
- Rançons ;
- Frais de reconstitution de données / assistance informatique ;
- Dépenses pour reprendre l'activité (dont demande pour nouvel agrément) ;
- Autres ???

Les couvertures envisagées

- Pertes d'exploitation ;
- Duplication des données à partir de sauvegardes existantes ;
- Reconstitution des pertes de données (sous réserve …) ;
- Pertes immatérielles suite à remise en question de l'agrément ;
- Frais de reconfiguration des systèmes ;
- Assistance informatique ;
- Recherche de cause
  - Frais de résolution
  - Frais de « mise en conformité ».

Les couvertures proposées

- Frais liés à la perte d'agrément et à la demande d'un nouvel agrément ?
- Paiement de la rançon ? / Frais mis en œuvre pour la payer ?
- Remboursement des pénalités contractuelles ?
- Remboursement des pénalités administratives ?
- Frais de gestion de crise ?
- Biens intangibles : Réputation, R&D …..
- Autres ??...

Pour quelles limites de couverture

Garanties		Limites
Pertes d'exploitation	1	
Reconstitution des pertes de données	2	
Pertes immatérielles suite à remise en question de l'agrément	3	
Frais de reconfiguration des systèmes	4	
Frais liés à la perte d'agrément et à la demande d'un nouvel agrément	5	
Assistance informatique	6	
Recherche de cause	7	
Paiement de la rançon	8	
Frais mis en œuvre pour la payer	9	
Remboursement des pénalités contractuelles	10	
Frais de notification	11	
Remboursement des pénalités administratives	12	
Frais de gestion de crise	13	
Biens intangibles : Réputation, R&D	14	
Carence de fsseur / client suite à évènement cyber chez le tiers	15	

Figure 7 – Garanties et limites de couverture

Regroupement par paquets de garanties

Les assureurs ont identifié les garanties qui pouvaient être mobilisées sur les segments des TPE et TPME – l'organisation des garanties étant différentes selon les sociétés d'assurance, la FFA a proposé dans l'intérêt de la recherche une nomenclature par paquet de garanties. Ont été sortis du champ de la réflexion car estimés non pertinents dans le cadre de cet exercice, les frais de notification sur les données personnelles, les pénalités administratives et les biens intangibles par souci de simplification car, à ce jour, les couvertures d'assurance sont rares en la matière.

Première colonne – gestion de crise, frais de gestion de crise, reconfiguration des systèmes, assistance informatique, recherche de cause, la reconstitution des pertes de données. Le second parquet réunit tout ce qui est adossé aux pertes d'exploitations et assimilé – pertes d'exploitation, frais liés à la perte d'agrément, pertes immatérielles et remboursement des pénalités contractuelles. Un troisième paquet est lié à la rançon, au paiement et ou frais de mise en œuvre. Le 4e paquet traite les carences fournisseurs / clients.

- Paquet 1 : garanties liées à la gestion de crise, appliquées dans les premiers jours après l'évènement (pendant 4 jours environ)
  - Reconstitution des pertes de données ;
  - Frais de gestion de crise ;
  - Frais de reconfiguration des systèmes ;
  - Assistance informatique ;
  - Recherche de cause

- Frais de résolution
- Frais de « mise en conformité ».

Remarque : Certains adhérents ont estimé le montant de ces garanties à environ 1 500 € / ETP / jour.

- Paquet 2 : les garanties liées aux pertes d'exploitations et assimilées
  - Pertes d'exploitation
  - Pertes immatérielles suite à remise en question de l'agrément
  - Frais liés à la perte d'agrément et à la demande d'un nouvel agrément
  - Remboursement des pénalités contractuelles
- Paquet 3 : garanties liées à la rançon
  - Paiement

    et/ou
  - Frais mis en œuvre ou engagés.
- Paquet 4 : garanties liées aux carences
  - Carence du fournisseur suite à un évènement cyber chez un tiers

    et/ou
  - Carence du client suite à un évènement cyber chez un tiers

Les garanties frais de notification, pénalités administratives et biens intangibles n'ont pas été retenues.

Ce tableau a été envoyé à l'ensemble des membres du GT cyber de la FFA pour réponse concernant les limites de capitaux et franchises. Taux de réponses intéressant – 7 des assureurs principaux français et anglo-saxons soit 70-80% du marché.

Estimation des limites et franchises par paquet de garanties

Garanties	Regroupement des garanties	Limites de capitaux (1)	Franchise (1)
Reconstitution des pertes de données	Paquet 1 : Garanties liées à la gestion de crise		
Frais de gestion de crise			
Frais de reconfiguration des systèmes			
Assistance informatique			
Recherche de cause (frais de résolution et/ou frais de mise en conformité)			
Pertes d'exploitation	Paquet 2 : Garanties liées aux pertes d'exploitation et assimilées		
Frais liés à la perte d'agrément et à la demande d'un nouvel agrément			
Pertes immatérielles suite à remise en question de l'agrément			
Remboursement des pénalités contractuelles			
Rançon : paiement et/ou frais de mise en œuvre	Paquet 3 : Garanties liées à la rançon		
Carence de fournisseur suite à un évènement cyber chez un tiers	Paquet 4 : Garanties liées aux carences		
Carence du client suite à un évènement cyber chez un tiers			

Figure8 – limites et franchises par paquet de garanties

VII.4.b. Le donneur d'ordre

Quels préjudices ?

Le secteur aéronautique européen est porté par le constructeur *Skyfleet*, et son modèle phare le *Skyfleet* S410. La flotte de ce modèle se compose de 2560 avions moyen-courrier en service dans le monde. 1000 avions sont en commande de par le monde à cette date. A titre indicatif, le prix moyen d'un *Skyfleet* S410 est de 100M€.

La production des avions est directement impactée à partir du mois de décembre 2018 et cela se traduit par :

- une baisse des cadences de l'ordre de 10% sur 3 mois ;
- une impossibilité de livrer une vingtaine d'avion sur la période.

Au regard des garanties contenues dans les contrats DaB

En l'absence de dommages matériels, la situation décrite relèverait de la catégorie des « *Non Damage Business Interruption* » (NDBI) qui soulève, dans le cas présent, au moins deux questions sur l'assurabilité :

- Des conséquences de la perte d'agrément d'un fournisseur ou d'un sous-traitant ;
- Des carences de fournisseur sans dommage.

Autres conséquences dommageables

- Pénalités contractuelles ;
- Frais éventuels de stockage des avions coût de location d'avions ?
- Dépenses pour reprendre l'activité ;
- ….

VII.5. Approche RC du scenario

VII.5.a. Origine de l'attaque

ATTAQUE MALVEILLANTE

L'attaquant utilise une faille de configuration des ERP afin d'accéder via un accès distant de maintenance.

En utilisant cet accès, il active une fonction native du système permettant de chiffrer les données de celui-ci.

ORIGINE de l'ATTAQUE

Soupçons de motivations géopolitiques et économiques

+

Utilisation d'un défaut de configuration des ERP imputé à un défaut d'installation et d'exploitation = Installation et exploitation des ERP externalisées à la société SG3.

+

Attaque par *ransomware* via un fournisseur (avant propagation) = Fournisseur identifié.

Eventuellement, le fournisseur du logiciel ainsi que les sociétés en charge de la maintenance de ces logiciels peuvent être impacté en adossement à leur garantie RC dans le cadre d'un recours. Ont été identifiées, les

entreprises qui avaient facilité la transmission du virus et qui pouvaient éventuellement subir un recours. Cependant, les capitaux peut-être nécessaires n'ont pas été identifiés parce que très faibles par rapport à de la RC pro.

VII.5.b. Schéma de mise en jeu des RC

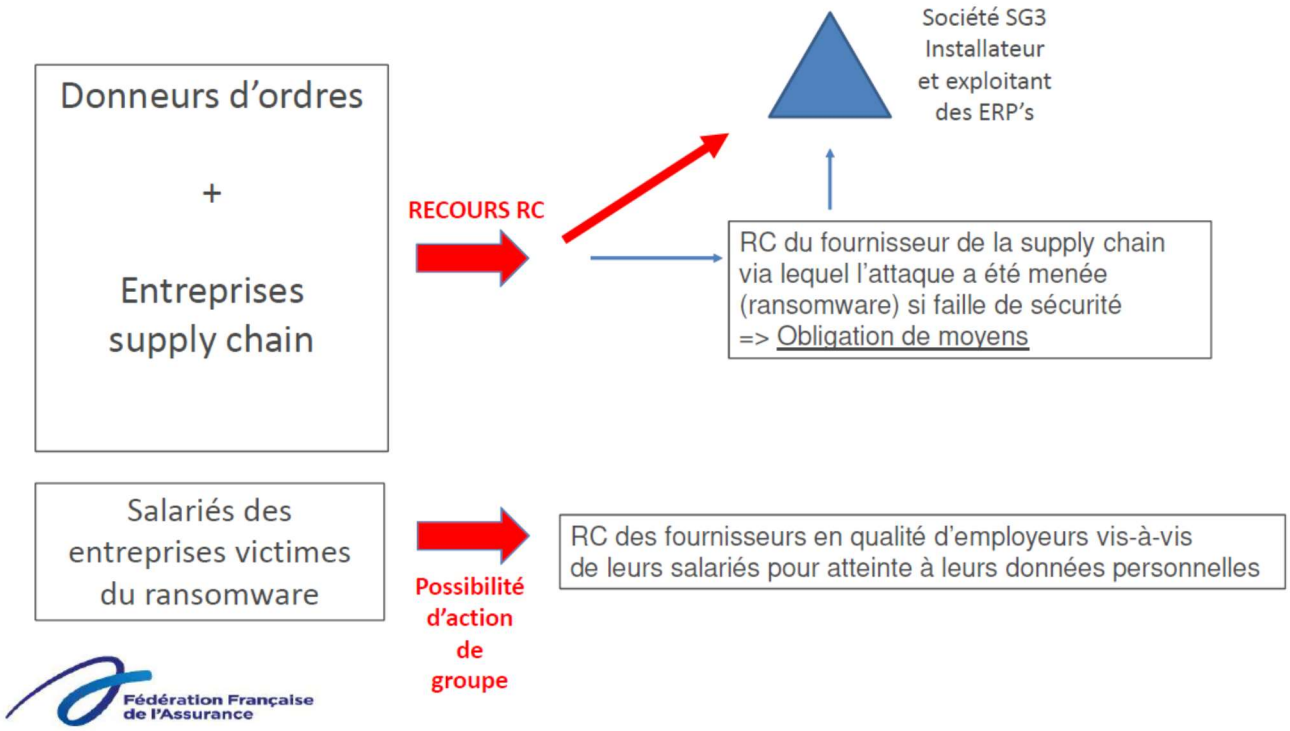


Figure 9 – Schéma de mise en jeu des RC

VII.5.c. Chaine des responsabilités

Selon le scénario, un seul prestataire a été en charge de l'installation de l'ERP. Se pose la question de la mise en cause de sa responsabilité par les fournisseurs impactés et quelles pourraient être les actions intentées en responsabilité.

Dans le cadre de l'exercice, l'hypothèse des RC croisées entre fournisseurs a été écartée. Il serait intéressant néanmoins de poursuivre le travail de réflexion afin d'étudier la chaine des responsabilités, les recours possibles des fournisseurs entre eux en cas de non-respect d'une obligation de moyen d'un niveau de cyber sécurité moyen en regard du suivi des standards *BoostAerospace Bronze*, *Silver* et *Gold*. En quoi une entreprise non conforme aux standards de *BoostAerospace* a-t-elle favorisé le sinistre ? L'objectif de recherche des frais partagés pourrait également se heurter aux considérations économiques de faire un recours. Actuellement, les montants de garantie disponible sur le marché ne sont pas à la hauteur des enjeux.

RC du fournisseur de la *supply chain* via lequel l'attaque a été menée (*ransomware*)

Le résultat final des investigations est parvenu à décrire précisément comment l'attaque a été menée et via quel fournisseur.

- Faille de sécurité chez ce fournisseur ?

- Mise en jeu possible de sa RC.

RC de la société en charge de l'installation et de l'exploitation des ERP = Société SG 3

Après 1 semaine d'investigations, les intrusions dans les ERPs ayant conduit à la mise en place de l'attaque peuvent être imputés à un défaut de configuration de ceux-ci lors de leur installation et exploitation. Une grande majorité des entreprises touchées avaient externalisées l'installation et l'exploitation de leur ERP à la société SG3.

- Faille de configuration des ERP imputable à l'installation et à l'exploitation des ERPs.
- Mise en jeu possible de sa RC Pro de la société SG3.

RC des fournisseurs en qualité d'employeurs vis-à-vis de leurs salariés

Si les ERPs contiennent des données personnelles, la RC de l'employeur peut être mise en jeu par les salariés en cas de divulgation de leurs données personnelles. Leur préjudice peut être un préjudice moral.

- Faille de sécurité chez les fournisseurs ?
- Mise en jeu possible de sa RC.

VII.5.d. Victimes et préjudices

Fournisseurs

TYPE A = 1 semaine d'arrêt de production (Pertes d'exploitation)

TYPE B = 15 jours d'arrêt de production + 20% de baisse de rendement de production pendant 1 mois.

- Remise en question du POA par l'ASA impliquant un surcoût de production de 10% ;
- => Pertes d'exploitation.

TYPE C= Perte du POA par l'ASA / Retour de la capacité de production sous 6 mois

- => Pertes d'exploitation

- + Pénalités contractuelles ;
- Rançon ;
- Préjudice d'image + gestion de crise ;
- Atteintes aux données personnelles notamment des salariés / Frais de notification ;
- Frais de reconstitution de données / assistance informatique.

Constructeur

Impossibilité de livrer une vingtaine d'avions (prix moyen/avion = 100Meuros) ;

Perte de marge brute 20% avec décote appliquée pour décalage de production ;

Préjudice d'image ;

Gestion de crise ;

L'exercice n'a pas porté sur les impacts constructeurs.

Compagnies aériennes

Préjudices économiques des compagnies aériennes

- Question de l'impact sur la garantie RC professionnelle aéronautique : la garantie RC professionnelle aéronautique ne devrait pas être concernée car elle ne couvre que le défaut du produit et non les pertes liées au retard de production.
- A noter que la garantie « *Grounding non-occurrence* » portant sur des avions en exploitation (et non en cours de fabrication) n'aurait pas vocation à jouer.

L'exercice n'a pas porté sur les recours potentiels des compagnies aériennes.

Autres donneurs d'ordres

D'autres donneurs d'ordres peuvent être victimes collatérales si les fournisseurs de la *supply chain* travaillent par ailleurs pour d'autres filières.

VII.5.e. Impacts sur les contrats

Pluralité de victimes :

- Sinistre sériel ?
  - ❑ 1 même cause technique ou plusieurs causes techniques (L142-1-1 CA) ?
    - ➢ Globalisation du sinistre sur une année d'assurance / Un plafond de garantie ?

Polices impactées ?

- ➢ RC Pro de la société en charge de l'installation et de l'exploitation des ERP - SG3 ;
- ➢ RC du/des fournisseurs de la *supply chain* en cas de faille de sécurité ;
- ➢ D&O chez certains des gros sous-traitants (préjudice des actionnaires) ;
- ➢ RC Atteintes aux données personnelles des salariés.

Impact : *Silent cover* ? Police Cyber / garantie dédiés ?

- ➢ Question de l'Impact sur le contrat RCG/Cyber de la SSII (Société SG3):
  - Clause contractuelle exclusive ou limitative de RC ?
  - Exclusion dans le contrat RCG ? *Silent cover* ?
  - Garanties impactées ? RC Pro /DINC ;
  - Montant de garantie limité ;
  - Question des pénalités contractuelles.
- ➢ Le temps des recours n'est pas celui de la résilience de la *supply chain*.
- ➢ Toutefois, nécessité pour les acteurs de la *supply chain* de disposer d'une garantie/contrat CYBER avec un volet responsabilité civile.

VII.6. Approche DaB du scenario

Quels préjudices ?

Les contrats de dommage aux biens peuvent également être mobilisés en cas d'attaque cyber.

- Dans le cadre de l'exercice nous avons estimé que les assureurs n'avaient pas identifié les couvertures susceptibles de jouer et donc leurs niveaux d'engagement (couverture silencieuse)
- Cette quantification sera réalisée par l'approche des ré assureurs.

VII.7. Estimation du coût total chez les fournisseurs

Estimation des limites et franchises par paquet de garanties (1) pour les TPE/PME: 7 réponses dont les 4 principaux français et 3 anglo-saxons

Garanties	Regroupement des garanties	Limites de capitaux (1)	Franchise (1)
Reconstitution des pertes de données Frais de gestion de crise Frais de reconfiguration des systèmes Assistance informatique Recherche de cause (frais de résolution et/ou frais de mise en conformité)	Paquet 1 : Garanties liées à la gestion de crise	1 500 000 €	1 500 €
Pertes d'exploitation Frais liés à la perte d'agrément et à la demande d'un nouvel agrément Pertes immatérielles suite à remise en question de l'agrément Remboursement des pénalités contractuelles	Paquet 2 : Garanties liées aux pertes d'exploitation et assimilées	1 000 000 €	12h
Rançon : paiement et/ou frais de mise en œuvre	Paquet 3 : Garanties liées à la rançon	325 000 €	2 500 €
Carence du fournisseur suite à un évènement cyber chez un tiers Carence du client suite à un évènement cyber chez un tiers	Paquet 4 : Garanties liées aux carences	1 000 000 €	24 h

Fédération Française de l'Assurance

Figure 10 – Estimation des limites et franchises par paquet de garanties

Les hypothèses

1. Périmètre: les TPE / PME
   - Pas d'estimation de capitaux assurés pour les hauts de segments ETI / GC
2. Reprise des hypothèses concernant les pertes des entreprises A, B et C,
   - Entreprise A: 60 % du total des Entreprises
     - réussissent à relancer leur ERP sous 1 semaine ➔ 1 semaine d'arrêt de production
   - Entreprise B: 20 % du total des entreprises
     - 15 jours d'arrêt de production, puis 20% de baisse de rendement de production pendant 1 mois

- Perte de toutes les données gérées par l'ERP (les informations de configuration de production) et notamment de production sur la période manquante, toutefois certaines informations papiers restent disponibles
- Remise en question du POA (*Production Organisation Approval*) par l'AESA (Agence Européenne de Sécurité Aérienne) impliquant un surcoût de production de 10%

▪ Entreprise C: 20 % du total des entreprises

- Retour à la capacité de production sous 6 mois
- Perte de toutes les données gérées par l'ERP (les informations de configuration de production) et notamment de production à compter du 1er novembre. Toutefois certaines informations papiers restent disponibles
- Obligation de reconfigurer entièrement le système
- Perte du POA

3. Taux de souscription de contrats cyber : 100 %
4. Périmètre des sous-traitants : 1.800
5. Taux d'entreprises touchées: 11 %
6. Coefficient majorant pour prise en compte des garanties supplémentaires du « paquet PE »
7. 30 % des entreprises sollicitent l'aide au paiement de la rançon
8. Non prise en compte des franchises

Pertes d'exploitation : Hypothèses

Entreprise de la supply chain	1800
Entreprises infectées:	11%
Entreprises assurées:	100%

Taille entreprise	Chiffre d'affaires (M€)	% d'entreprises de la supply par CA	Nombre d'entreprises de la supply chain	Nombre d'entreprises infectées	Nombre d'entreprises assurées	Nombre d'entreprises par type de conséquences		
						A 60%	B 20%	C 20 %
Big Groups	>500	3,75%	68	7	7	4	1	1
	200-500	3,75%	68	7	7	4	1	1
	100-200	6,25%	113	12	12	7	2	2
	50-100	12,50%	225	25	25	15	5	5
Mid Size	10 à 50	43,75%	788	87	87	52	17	17
SME	<10	30%	540	59	59	36	12	12
			1800	198	198	119	40	40

Figure 11 – caractérisation des entreprises de la filière

	Chiffre d'affaires moyen (M€)	Coeff d'atténuation de la PE (présence de back-up, continuité d'activité, travail en mode dégradé…)	Taux de marge brute moyen (%)	Catégories B Durée de l'arrêt de production (jours)	Catégories B Baisse de rendement	Catégories B Durée de la baisse de rendement (jours)	Catégories C Retour de la capacité de production (jours)
Big groups	750	10%	20%	15	20%	30	90
	350	8%	20%	15	20%	30	100
	150	6%	20%	15	20%	30	110
	75	5%	20%	15	20%	30	130
Mid size	30	3%	20%	15	20%	30	150
SME	5	0%	20%	15	20%	30	180

Figure 12 – pertes d'exploitation

Pertes d'exploitation: Formule de calcul

Entreprise A : 1 semaine d'arrêt de production.

- CA moyen* (1-coef d'atténuation de la PE)* taux de MB divisé par 52 semaines (1 semaine d'arrêt)

Entreprise B : 15 jours d'arrêt de production, 20% de baisse de rendement de production pendant 1 mois. Remise en question de la certification de(s) avion au niveau Avionneur (POA) par l'agence de certification (EASA), augmentation des couts de production pour l'entreprise fournisseur de 10%.à étayer revalider/ cause-conséquences.

- CA moyen* (1-coef d'atténuation de la PE)*taux de marge brut * durée de l'arrêt de production divisée par 365 jours + CA* taux de MB*(1-baisse de rendement) * nombre de jours d'arrêt / 365

Entreprise C : Perte du POA par l'EASA coté Avionneur, retour de la capacité de production sous 6 mois.

- CA moyen* (1-coef d'atténuation de la PE)* taux de MB * nombre de jours d'arrêt de prod. / 365

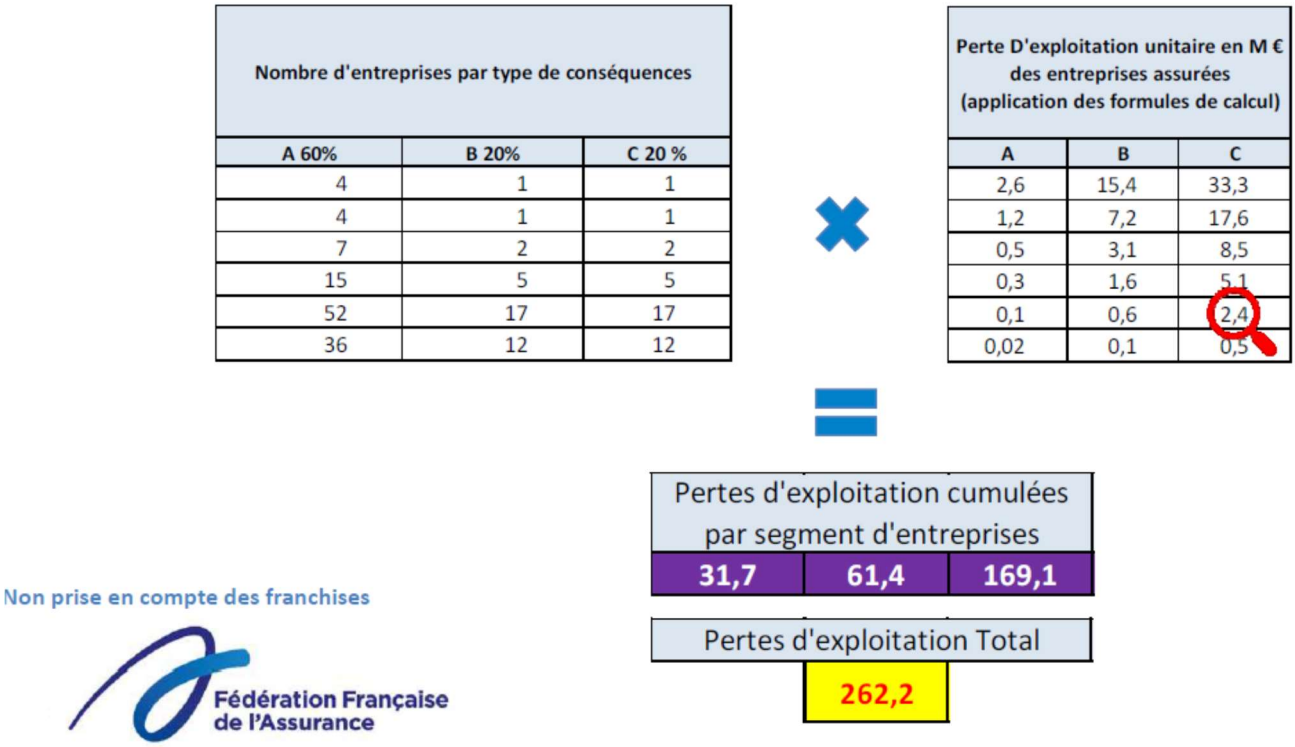


Figure 13 – pertes d'exploitation cumulées par segment d'entreprises

La pastille rouge concerne les TPE, le chiffre de 2,4M se situe au-dessus des couvertures délivrées actuellement.

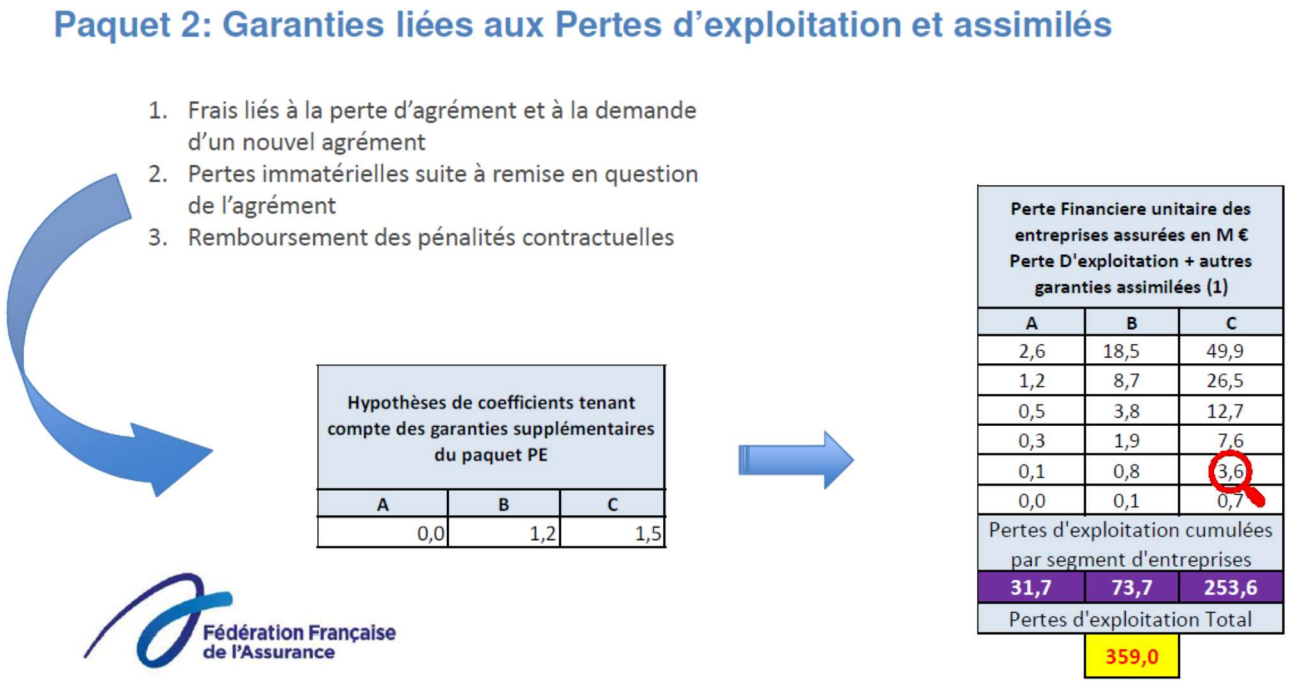


Figure 14 – garanties liées aux pertes d'exploitation et assimilés

Gestion de crise

1. Plafond de garantie moyen 1.500.000 € pour les PME / Estimation à dire d'expert pour les GC
2. Hypothèse de consommation de la garantie

Taille entreprise	Chiffre d'affaires (M€)
Big Groups	>500
	200-500
	100-200
	50-100
Mid Size	10 à 50
SME	<10

Figure 15 – typologie d'entreprises

Nombre d'entreprises par type de conséquences			Hypothèse de consommation de la garantie			Coût unitaire		
A 60%	B 20%	C 20 %	A	B	C	A	B	C
4	1	1	0%	0%	50%	39 000	150 000	750 000
4	1	1	0%	0%	50%	29 250	112 500	562 500
7	2	2	0%	5%	75%	18 000	75 000	375 000
15	5	5	5%	10%	75%	7 500	30 000	150 000
52	17	17	5%	10%	50%	74 925	149 850	749 250
36	12	12	10%	20%	50%	149 850	299 700	749 250
						Coût par segment d'entreprise		
						9 783 960	6 880 525	25 501 534
						Coût total		
							42 166 018	

Figure 16 – coût par segment d'entreprise

Synthèse

1. Base de 1 800 fournisseurs / 11 % de touchés / 100 % assurés
2. Autres hypothèses pas garanties (voir ci avant)
3. Sans prises en compte des carences, biens intangibles et frais de notification

Pertes d'exploitation	Et assimilées	Aide aux paiement de la rançon	Frais de Gestion de crise
262 198 657 €	96 829 323 €	18 531 563 €	42 166 018 €
419 725 561 €			

Figure 17 – synthèse des coûts

1. Base de 1 800 fournisseurs / 25 % de touchés / 100 % assurés

Pertes d'exploitation	Et assimilées	Aide aux paiement de la rançon	Frais de Gestion de crise
595 906 039 €	220 066 644 €	42 117 188 €	95 831 859 €
953 921 730 €			

2. Base de 1 800 fournisseurs / 50 % de touchés / 100 % assurés

1 191 812 079 €	440 133 288 €	84 234 375 €	191 663 719 €
1 907 843 460 €			

3. Base de 15 000 fournisseurs / 11 % de touchés / 100 % assurés

2 184 988 811 €	806 911 027 €	154 429 688 €	351 383 484 €
3 497 713 010 €			

4. Base de 15 000 fournisseurs / 25 % de touchés / 100 % assurés

4 965 883 660 €	1 833 888 699 €	350 976 563 €	798 598 828 €
7 949 347 750 €			

Figure 18 – synthèse des coûts sous diverses hypothèses

Mise en perspective avec le coût des sinistres climatiques

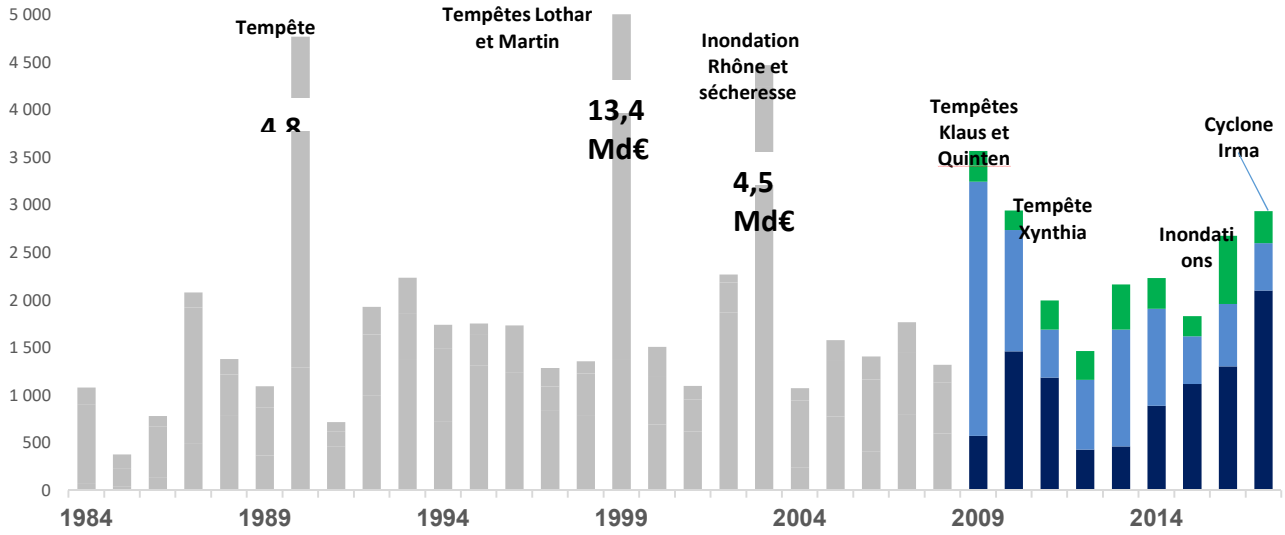


Figure 19 – En France : historique des événements naturels majeurs depuis 1984

VII.8. Estimation du coût total chez le donneur d'ordre

Au regard des garanties contenues dans les contrats DaB…

En l'absence de dommages matériels, la situation décrite relèverait de la catégorie des « *Non Damage Business Interruption* » (NDBI) qui soulève, dans le cas présent, au moins deux questions sur l'assurabilité :

Des conséquences de la perte d'agrément d'un fournisseur ou d'un sous-traitant.

Des carences de fournisseur sans dommage.

Autres conséquences dommageables

- Pénalités contractuelles ;
- Frais éventuels de stockage des avions cout de location d'avions ?
- Dépenses pour reprendre l'activité.

VII.9. Synthèse assurance

Un cout estimé à

- 420 M€ en fourchette basse
- 1,9 M€ en fourchette moyenne
- 8 M€ fourchette haute,
  - Sans tenir compte du coût assuré pour le donneur d'ordre;
  - Sans tenir compte des conséquences dommageables sur les autres filières en cas d'attaque diffuse (non ciblée vers la seule filière aéronautique);
  - Sans tenir compte de l'estimation du cout lié à la mise en jeu du/des contrats de RC;
  - Sans tenir compte des *silent covers* en DaB.

VIII. Réponse de la Réassurance et de l'APREF

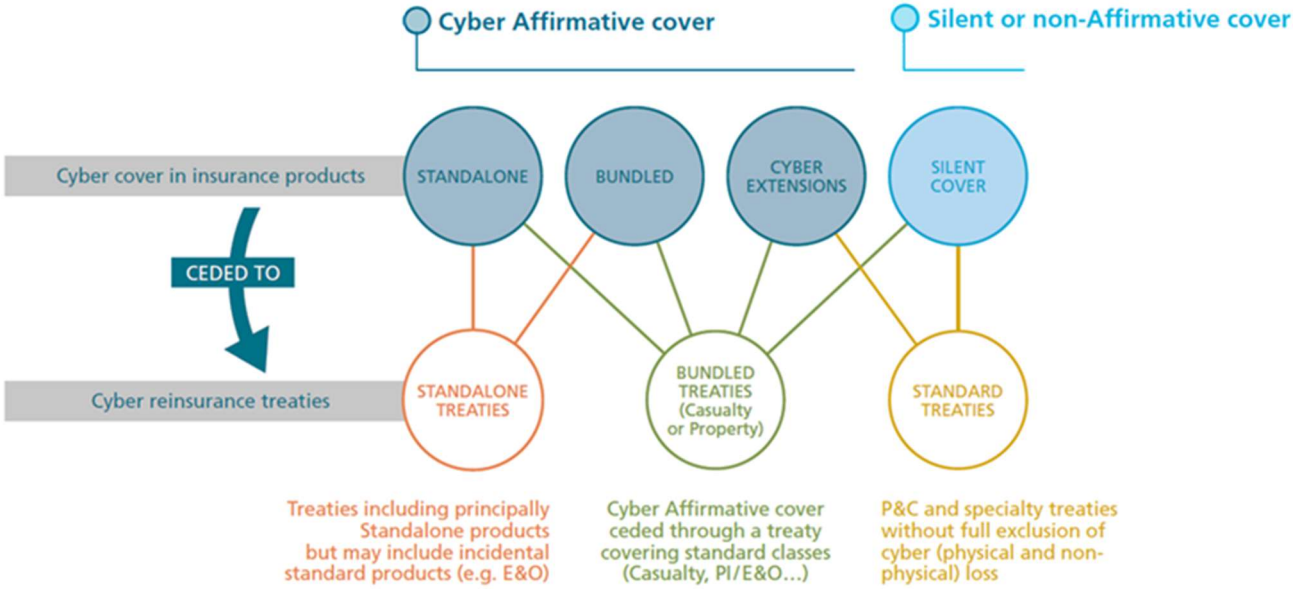


Figure 20 – Transfert vers la réassurance

VIII.1. Garanties & Traités : Exposition en termes de réassurance, quantification

VIII.1.a. Hypothèses sur le marché Cyber

Estimation des primes spécifiques Cyber (en millions EUR)	2017
Marché Français	50
Europe	200
Monde	3'500

Figure 21 – Le marché de la cyber-assurance en 2017

VIII.1.b. Hypothèse du scénario (polices Cyber uniquement)

1. Base de 1 800 fournisseurs / 11 % de touchés / 100 % assurés
2. Autres hypothèses pas garanties (voir ci avant)
3. Sans prises en compte des carences, biens intangibles, frais de notification

1er exercice, un regard porté sur les contrats et les garanties et la quantification du scénario sur le monde de la réassurance, à partir des données FFA.

2nd exercice, les challenges à relever pour le développement de l'assurance du risque cyber. Le secteur de la réassurance va assumer une grande partie du coûté économique du sinistre assuré : il souhaite avant tout maitriser ses engagements et équilibrer ses résultats.

419M calculés par la FFA, l'APREF s'est basée sur le sinistre raisonnable – sur la base de 18000 fournisseurs, 11% touchés, 100% assurés.

Pertes d'exploitation	Et assimilées	Aide aux paiement de la rançon	Frais de Gestion de crise
262 198 657 €	96 829 323 €	18 531 563 €	42 166 018 €
419 725 561 €			

Figure 22 – quantification finale du scénario DOBYCHA

VIII.1.c. Scénario qui déclenche essentiellement des garanties Cyber spécifiques

Une première analyse de sévérité du scénario consiste à considérer le rapport Sinistre/Prime, indicateur intuitif très utilisé par les réassureurs. Il en ressort :

S/P d'un tel évènement pour le Marché Français : 419M / 50M soit 838%

Période de retour induite: 9 ans sur le marché français. L'intégralité de 9 ans de primes du marché français est donc nécessaire pour payer un tel sinistre et ce, sans la survenance d'aucun autre évènement cyber d'aucune sorte (nous rappelons que les assurés du scénario sont basés en France).

S/P d'un tel évènement pour le Marché Européen: 419M / 200M soit 210%

Période de retour induite : 2 ans

Si on se limite à la filière aéronautique uniquement et en partant d'une estimation relativement optimiste en termes de montant de prime moyenne :

- Prime moyenne estimée à 5000 euros pour les 1800 entreprises
- Prime totale : 9M euros
- S/P d'un tel évènement pour la filière : 419M / 9M soit 4655%
- Période de retour induite : 46 ans

La probabilité d'un tel scénario nous apparaît pourtant beaucoup plus importante au regard des différentes discussions : le marché est encore immature, les montants de primes insuffisants pour pallier les sinistres futurs et la prise de conscience doit continuer à se développer.

VIII.1.d. Assurance - Garanties impactées par le scénario

- Polices spécifiques cyber (*First party & Third party*) -> pris en compte par FFA
- Polices non-spécifiques cyber
  - Perte d'exploitation sans dommage direct des polices dommages ;
  - D&O chez certains des gros sous-traitants ;
  - RC Atteintes aux données personnelles des salariés ;
  - RC du/des fournisseurs en cas de faille de sécurité - dans et hors filière aéronautique ;
  - RC Pro de la société en charge de l'installation et de l'exploitation des ERP - SG3.

Ces couvertures sont susceptibles de participer à la valorisation du sinistre assuré : il nous semble important de les identifier et de les mentionner car elles n'ont pas fait l'objet d'une quantification dans le cadre de notre sinistre raisonnable.

VIII.1.e. Hypothèses pour la quantification Réassurance

- Contrats Cyber : 10 assureurs
  - 9 Traités Quote-Part (réassurance proportionnelle) (taux de cession entre 50% et 90%) – Hypothèse : pas de limites par évènement ;
  - 1 traité « *Stop-Loss* » (réassurance non-proportionnelle basée sur le ration sinistre/primes avec des paramètres : 800% XS 200% de primes (sur la base de la prime moyenne). Ces paramètres moyens ne reflètent pas la très grande hétérogénéité sur le marché (indicateur d'une certaine immaturité) où l'on trouve des paramètres allant de 80% à 79% pour la rétention et de 20% à 1500% pour la limite
- Non retenu pour l'exercice :
  - Traités « *Excess* par risque ») : 4 polices concernées pour un montant réassuré de 70M euros ;
  - Traités « *Excess* par évènement ».
- Autres contrats pouvant être touchés par le scénario
  - Polices Dommages ;
  - Polices RC ;
  - Polices *Kidnapp&Ransom* ;
  - Polices RC des mandataires sociaux (RCMS).

VIII.1.f. Traités Cyber

MONTANT TOTAL ASSURE (CYBER)	**419 725 561 €**					
Nombre d'entreprises dans la filière	1 800					
Pourcentage infection	11%					
Nombre d'entreprises infectées	198					
Prime moyenne (€)	5 000					
Prime totale marché FR (€)	50 000 000					
Nombre de cédantes marché FR	10					
Traités Cyber						
		Taux de cession				
Traités Quote-Part	50%	60%	70%	80%	90%	
Réassuré	209 862 781 €	251 835 337 €	293 807 893 €	335 780 449 €	377 753 005 €	
Nombre de traités QP	10					
Taux de cession moyen	70%					
Montant réassuré moyen	**29 380 789 €**					
	Retention en % du S/P	Limite en % du S/P				
Stop-Loss	200%	800%				
S/P moyen en FR	839%					
Encaissement moyen par cédante	5 000 000					
Part moyenne du sinistre par cédante	41 972 556					
Application traité	10 000 000	40 000 000				
Montant réassurance	**30 000 000 €**					
Réassurance						
QP	9					
Stop-loss	1					
TOTAL Réassurance	**294 427 104 €**					

Figure 23 – quantification réassurance du scénario DOBYCHA

Un total d'environ 300M€

Soit 70% du sinistre assuré à la charge de la réassurance au titre des contrats Cyber.

VIII.1.g. Autres contrats : quantification du sinistre issu des polices « silencieuses »

A partir de la liste des garanties identifiées par la FFA comme pouvant être impactées par le scénario de la FFA, l'objectif a été ensuite d'ouvrir aux autres garanties susceptibles de fonctionner issues d'autres traités et d'autres lignes de business qui sont les Pertes d'Exploitation sans dommage direct matériel, des police dommage, la RC – atteinte aux données personnelles de salariés, la RC des fournisseurs et la RC pro de SG3. L'objectif était de montrer que l'estimation faite se basait sur un périmètre cantonné mais que, pour autant d'autres expositions existaient issues des couvertures susceptibles de jouer, pouvant modifier le chiffre final.

- Polices Dommages (seules chiffrées ci-dessous) ;
- Polices RC ;
- Polices K&R ;
- Polices RCMS ;

+35% de sinistre supplémentaire assuré…

Sous-limite moyenne police property	Montant Financier Perte D'exploitation + Reconstition de données		
	A	B	C
20	2,6	18,5	20,0
10	1,2	8,7	10,0
10	0,5	3,8	10,0
5	0,3	1,9	5,0
5	0,1	0,8	3,6
5	0,0	0,1	0,7
	31,7	73,7	165,0
15%	4,75	11,06	24,75
			40,56

Sous-limite moyenne police property	Montant Financier CBI
	A
10	10,0
5	5,0
5	5,0
2,5	2,5
2,5	2,5
2,5	2,5
	4856,1
1,5%	72,84
	72,84

Figure 24 – quantification du sinistre issu des polices « silencieuses »

Les *must have* pour la réassurance : clarification des garanties des polices d'assurances (CBI, Pertes sans Dommages).

Le sinistre pour la partie RC n'est pas estimé mais existe.

VIII.1.h. Total Réassurance

Hypothèse : 50% des sinistres des couvertures silencieuses sont cédées à la réassurance. Compte tenu des couvertures silencieuses, on estime à 113,4M le sinistre assuré additionnel. En estimant que 50% de ce nouveau montant est réassuré la charge finale pour les réassureurs se monterait à 350M.

QP	SL	Couvertures silencieuses
264 427 101 €	30 000 000 €	56 699 904 €
351 127 005 €		

Figure 25 – quantification totale du sinistre pour la réassurance

Soit 83% du sinistre assuré pour un scénario qui touche majoritairement des polices cyber spécifiques.

VIII.2. Problématique Réassurance: *silent covers*, clause de définition de l'évènement, accumulation

VIII.2.a. Les couvertures « silencieuses »

- NotPetya : 10% seulement de polices spécifiques (source : PCS). Environ $3B de coûts assurés, $10B de coût économique ;
- Besoin de clarifier les polices standards pour éviter les « mauvaises surprises » ;

- Nécessité de connaître les engagements pour accompagner le développement du marché de l'assurance Cyber ;
- Nécessité de tarifer ces couvertures.

Recommandation :

- Clarifier la réponse des polices standards aux événements cyber et tarifer les éventuelles couvertures cyber ;
- Sensibiliser au risque ce qui permettra valoriser l'investissement, l'achat d'une couverture d'assurance et de justifier du montant de la prime.

VIII.2.b. Agrégation / Accumulation

Un risque déjà particulier

- Sans frontière (enjeux systémique et problème de la mutualisation) ;
- Concentration des technologies IT et développement des objets connectés.

L'élargissement des polices cyber accroît la difficulté de gestion des cumuls

- Couverture des pertes dues à des carences fournisseurs et des clients ;
- Couverture des pannes ;
- Pertes de CA dues à un problème de réputation suivant un incident cyber ;
- *Bricking* (bris de machine sans dommage matériel nécessitant, par exemple, une reprogrammation et générant une perte financière).

Des modèles encore jeunes et des données encore insuffisantes

- Tarification perfectible ;
- Analyses des capacités (Pertes Maximales, Scenario,…) incertaines ;
- Allocation difficile du capital et des réserves (fortes contraintes règlementaires).

Les dommages cyber se diffusent dans de nombreux contrats

- Un incident peut toucher
  - Plusieurs assurés, liés ou non (*Supply Chain*/Carence Fournisseurs) ;
  - Plusieurs polices chez un assuré (Cyber, Dommages, RC, Fraude, RCMS, …).
- Plusieurs assureurs peuvent participer aux polices d'un assuré (grands risques)
- En réassurance, peuvent être touchés :
  - Plusieurs traités de lignes d'assurance différentes (même assureur) ;
  - qui peuvent être issus des couvertures affirmatives ou « silencieuses ».
- Plusieurs années de souscription impactées par un même évènement

L'emberlificotage des garanties, des sources d'exposition rend complexe l'analyse des accumulations et donc des expositions et freine inévitablement le développement du marché.

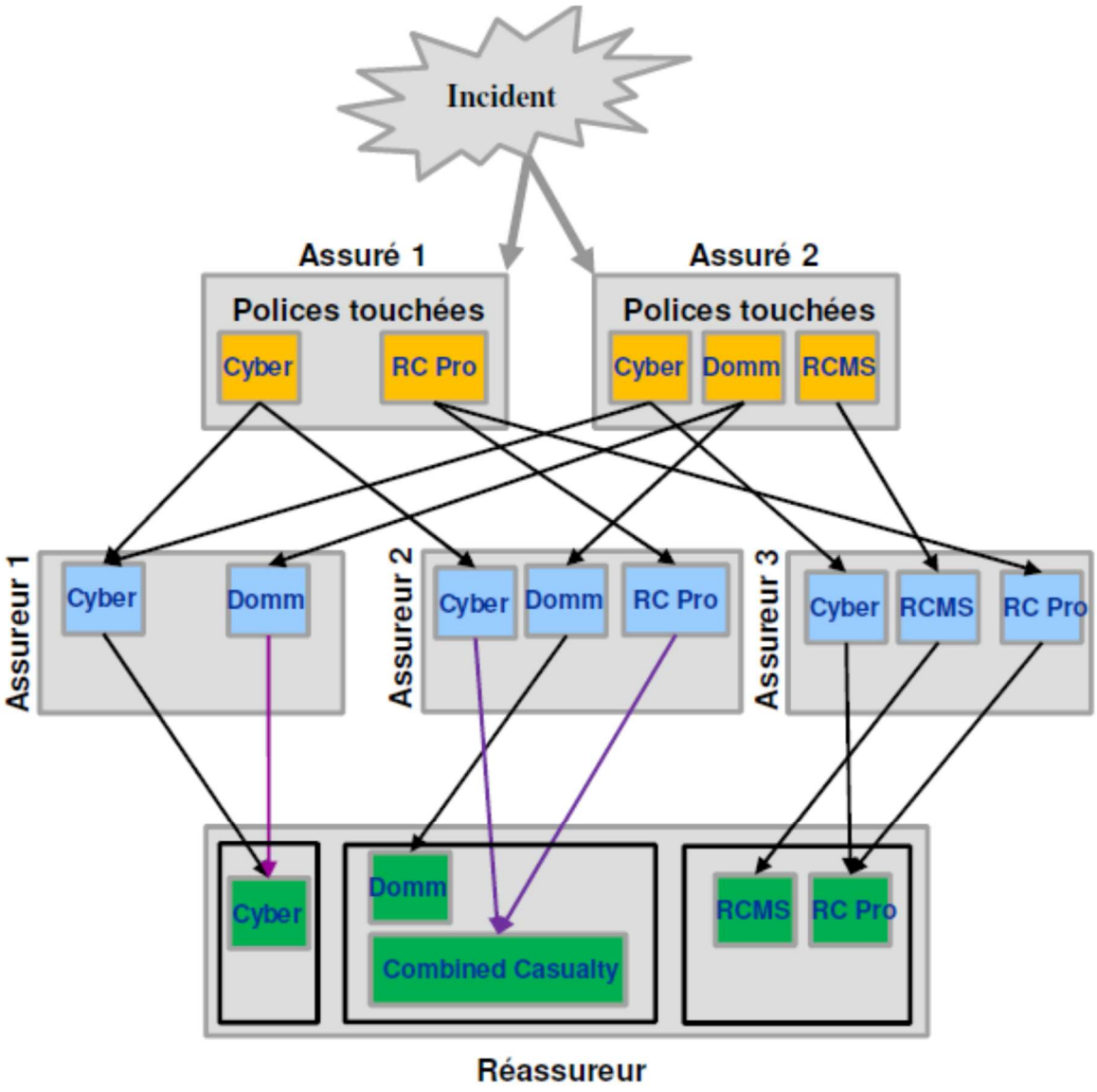


Figure 26 – Le problème des clashes

Recommandations au sujet des accumulations :

- Mise en place d'outils / de méthodes de calcul et de suivi des expositions
  - Modélisation (scénarios Cat Cyber, PML assuré et événement) ;
  - Clarification des polices pour réduire les possibilités de clash ;
- Prise de conscience du caractère systémique du risque Cyber.
  - Information et formation

VIII.2.c. La définition des événements cyber

Contrairement aux Catastrophes Naturelles, un événement cyber n'a pas de limite géographique, temporelle, causale.

Pourtant il y a besoin de délimiter les engagements sur un « événement » et de définir la couverture offerte.

Une définition des évènements Cyber est donc nécessaire - recherche de clauses pertinentes.

Aujourd'hui, quelques clauses existent, regroupant deux ou plus des critères ci-dessous mais elles ne semblent pas susciter une adhésion de l'ensemble des acteurs et peuvent apparaître parfois contestables en cas de sinistre…

- cause commune/ origine commune ;
- source commune / acteurs ou hackers ;
- clause horaire ;
- reconnaissance technique
  - Wannacry/Not Petya : 1 ou 2 évènements ? Selon les clauses, les réponses varient…

Recommandation :

- Travailler à une/des clauses robustes et reconnues

Difficultés complémentaires

- Rétrocession encore limitée ;
- Pertes non assurables : Perte de valeur des entreprises / intangibles mais la demande émerge ;
- Solidité des clauses, par exemple exclusion Guerre (Mondelez contre Zurich Insurance suite à Not-Petya – cf. Annexe 9).

Recommandations complémentaires:

- La formation de tous les acteurs de la chaine au risque réel

Thèmes	Recommandations	Destinataires
Clarté et robustesse des contrats	• Clarification des polices standards (dommage, RC) pour identifier et réduire les expositions « silencieuses » et les risques de clash • Revue juridique des clauses d'exclusions (e.g. exclusion Guerre) • Travailler à une/des clauses robustes et reconnues de définition d'événements	Assurés, assureurs, réassureurs
Développement et structuration du marché	• Améliorations des outils et méthodes de calcul et de suivi des expositions • En lien avec la clarification des polices, tarification des extensions Cyber des contrats standards.	Assureurs, réassureurs, régulateurs

Général	• Information et formation sur le risque Cyber pour:
	  • améliorer sa gestion et sa souscription
	  • valoriser l'investissement, l'achat d'une couverture d'assurance et de justifier du montant de la prime
		Tous

Figure 27 – Les recommandations issues de la réassurance

VIII.2.d. Conclusion

Scénario théorique mais crédible, avec une probabilité de survenance réelle.

Impact fort sur l'assurance mais surtout sur la réassurance.

La réassurance saurait assumer un tel évènement mais sa survenance ou celle d'un scenario similaire sur une autre filière aurait un impact fort sur le marché.

Et au regard des montants de sinistres, la prime d'assurance initiale pourrait apparaitre faible….

Pour un marché pérenne, il faut un marché spécifique, une prime de risque adaptée à une exposition maitrisée, un volume de prime suffisant pour mutualiser, une expertise des acteurs…

Les recommandations énoncées vont dans ce sens.

Annexe 1 – *BoostAerospace*

Le programme Air cyber de *BoostAerospace* a permis de fédérer Airbus Thales Safran et Dassault ainsi que d'autres industriels membres avec le support de l'ANSSI et du GIFAS pour élever le niveau de maturité de l'ensemble de la chaine aéronautique afin que les 2000 entreprises identifiées arrivent au même niveau de sécurité que leurs *Primes* d'ici 2023. Il est attendu que les entreprises arrivent à détecter des attaques, se protègent et souscrivent une assurance cyber. L'idée est d'arriver d'ici 4 ans à obtenir du marché une offre d'assurance cyber qui corresponde à un vrai risque avéré et un vrai dédommagement pour la filière aéronautique afin que la souscription d'assurance par les ETI PME ait un vrai sens en termes d'investissement financier.

La mission de *BoostAerospace* est de contribuer à l'élévation du niveau de sécurité de la chaine d'approvisionnement. Transfert le risque résiduel vers l'assurance est un des moyens de financer le risque. Dans le cadre du programme Air Cyber, *BoostAerospace* aide les entreprises partenaires à conduire un audit de maturité cyber sur la sécurité de leur système d'information et leur système industriel. *BoostAerospace* a lancé un POC sur l'assurance en 2017 auprès des grands donneurs d'ordre et des sous-traitants en diffusant des questionnaires techniques et portants sur l'assurance.

Les résultats du POC ont montré que les niveaux de maturité sont différents et que certaines entreprises sont capables d'identifier leur besoin d'assurance cyber et leur besoin de couverture d'autre pas encore. Les résultats montrent également que le projet d'assurance cyber pour la filière est réaliste et qu'il rencontre une vraie demande pour autant que qu'un travail de sensibilisation et de préparation soit entrepris dans le cadre d'un dialogue avec les entreprises.

L'attente de *BoostAerospace* est que le marché de l'assurance soit prêt d'ici 4 ans pour proposer des offres de couverture correspondant aux attentes de la filière. Les primes de la filière aéronautique, Airbus, Safran et Thales soutiennent cet exercice parce que si la chaine d'approvisionnement s'assure, ils s'assureront moins sur les risques cyber portés par la chaine d'approvisionnement.

Source : https://www.boostaerospace.com/aircyber/

AirCyber
Cybersecurity improvement of AeroSpace and Defense SupplyChain
The BackGround:

The AeroSpace and Defense Extended Enterprise is composed of multiple small and medium sized companies, having usually their ICT managed in silos without even the capability to detect that they are subject to cyber-attacks or to protect from those attacks.

One of the main issues to be resolved today is that those companies are the first target of cyber criminals while being the less protected.

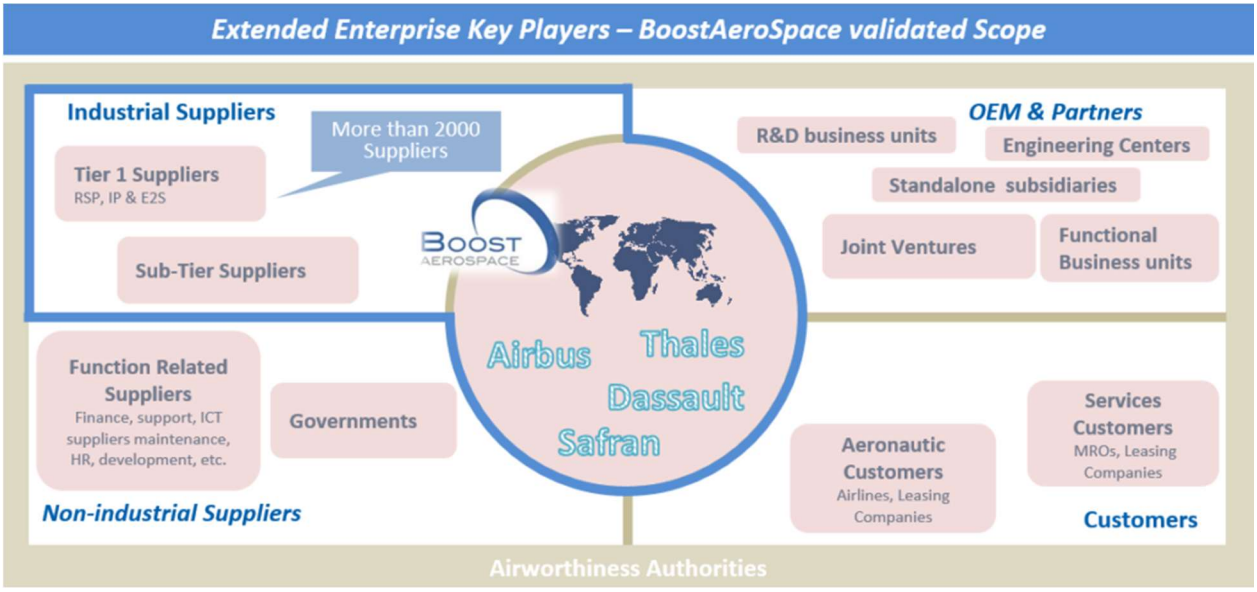
Over the past 5 years, the experience confirmed that attackers shifted their efforts to suppliers, as illustrated by multiple security issues reports like the one published by the UK Computer Emergency Response Team (CERT) in their white paper dedicated to "Cyber-security risks in the supply chain".

Unfortunately, while having spent a lot of efforts to secure their internal ICT, the security protections that BoostAeroSpace (BAS) founders (Airbus, Dassault Aviation, Safran, Thales) deployed inside their ICT are not deployed equally to their partners with whom they connect with to collaborate.

Therefore, in order to solve this urgent issue, BAS together with security specialists for Airbus, Dassault Aviation, Safran an Thales proposed to the Board of Directors (BOD) decide to launch together the AirCyber program.

Aim of the program:

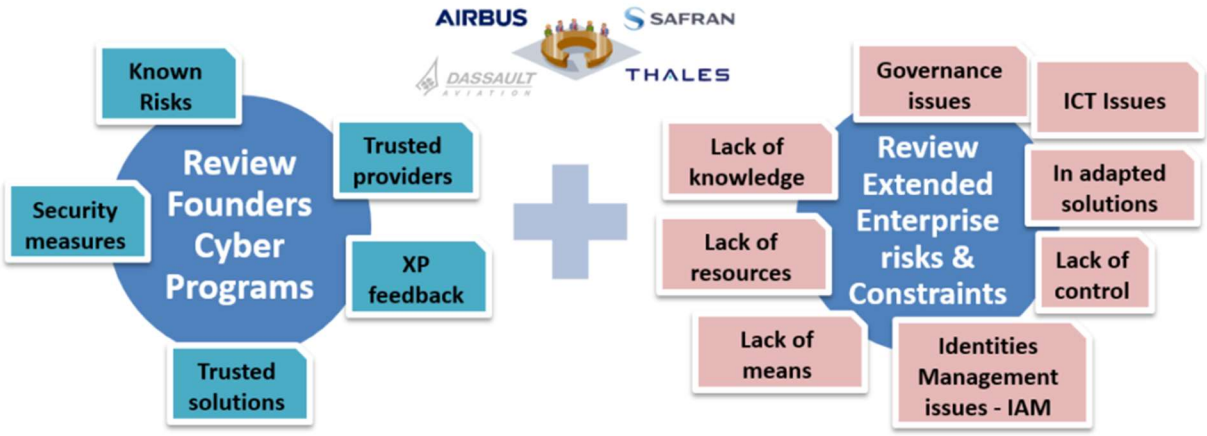
The agreed target of the program is to enhance security of the extended enterprise using BoostAeroSpace as a central Hub for BAS founders and other customer companies, and to propose security solutions for industrial suppliers first with a progressive approach.



Work performed: risks, issues, OEM inputs and solutions reviews

Security workshops were organized during one year with the key security representatives of the BAS founding companies (ie. Members of the BAS Security Management Authority, security experts appointed by BOD members and cyber security program managers).

Participants investigated what were the issues related to the collaboration in the extended enterprise and what would be the key success factor of a solution along with the risks of having a central approach on some sensitive domains like alerts management.



It was commonly agreed that BoostAeroSpace was well positioned to address some of the issues and that for some others it would not make sense to have a centralized approach, or would even increase the risk.

Solution concept and deliverables

The proposed solution consists in launching a cyber security program driven by BoostAeroSpace founders that will take all workshops inputs into consideration in order to achieve 2 main goals:

1. A BAS founders' centralized and shared standard to manage security of their supply chain extended enterprise (policies, tools and processes dedicated to Extended Enterprise security management validated by all founders).
2. A central hub of trusted security solutions and services proposed to the supply chain extended enterprise having done theirs proofs.

Major deliverables are organised as follow:

- AirCyber Continuous Maturity Assessment Services: On-site intervention to assist with the questionnaire, detailed safety report, renewed every 4 years. Update tool / Dashboard of levels.
- Cybersecurity Documentation (studies, configurations, and awareness) adapted from OEMs.
- A dynamic catalog of proposed trusted Cyber services and solutions recognized in the industry, with a rating system and offering the possibility to identify those services and solutions already referenced either by OEMS or industrial suppliers.
- A global awareness and collaboration CyberSecurity Plan (forums, events, etc.).
- A CyberSecurity issue detection and alerts solution fully compatible with OEMs and interconnected with international CyberSecurity databases.

Why AirCyber is the good answer?

Aerospace & Defense SupplyChain Extended Enterprise will find in AirCyber both trusted Industrial Control System and Information Technology security services and solutions to enhance their own security resilience and a structured referential to make their efforts and maturity level recognized by OEMs and customer companies.

Subscribing to the "AirCyber" service will allow them to benefit from:

- The CyberSecurity improvement plan led by the founders / shareholders of BoostAeroSpace (Awareness, analysis of your level of maturity, sharing of guides, best practices and expertise of the founders made available to them),
- The AirCyber dynamic catalog containing trusted CyberSecurity solutions and services updated and recognized by the Aerospace and Defense industry.

AirCyber has been officially launched in 2019!

The subscription is now available: we therefore invite industrial suppliers to join "AirCyber" in order to achieve the industry's standardization objectives for CyberSecurity protection as soon as possible.

Please note that we are committed to helping a defined number of suppliers each year, so the first subscription requests will automatically be included in the first wave 2019 of suppliers.

If you are a supplier, do not wait any longer and join AirCyber now by sending an email to

aircyber@boostaerospace.com

The AirCyber cybersecurity solutions and service catalog, that will be proposed to industrial suppliers is also opened. If you are a supplier of cybersecurity services or solutions to our shareholders or to industrial suppliers, do not hesitate to get in touch with us.

If you want to participate in this activity, as a supplier, service provider or partner, do not hesitate to contact us also with the same email address.

Annexe 2 – Bibliographie

Cette bibliographie couvre les principaux documents exploités lors de nos travaux année 3. Les deux premiers rapports comprennent également une annexe bibliographique, plus complète, qui n'est pas reprise ici.

Cyber Gouvernance

1. FERMA https://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy
2. Le Club des juristes https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_assurer-le-risque-cyber_janvier_2018_fr.pdf
3. SGDSN, *La revue de stratégique de cyberdéfense 2018,* http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

Cyber Assurance

1. *Insurance Europe,* "*Preparing for Cyber Insurance"*, october 2018, 28 pages , https://www.insuranceeurope.eu/preparing-cyber-insurance
2. A Moment of Truth for Cyber Insurance, février 2019, https://www.lawfareblog.com/moment-truth-cyber-insurance

Cyber Risque

1. CyRiM Report 2019, "*Bashe attack, Global infection by contagious malware"*, Nanyang Technological University – Insurance Risk and Finance Research Center including the Cambridge Centre for Risk Studies, les Lloyds, AON, MSIG, SCOR, TransRe, 2019, 77 pages https://www.lloyds.com/news-and-risk-insight/risk-reports/library/technology/bashe-attack
2. Moody's Investor service, Sector in Depth, "Credit Implication of Cyber will hinge on business disruptions, reputational effects' February 20189, 32 pages, https://www.moodys.com/research/Moodys-Credit-implications-of-cyberattacks-will-hinge-on-long-term--PBC_1161216

Annexe 3 – La lettre d'invitation

Madame, Monsieur,

Dans le cadre de son projet EIC[21] (Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité), l'IRT SystemX mène des travaux sur **la maîtrise du risque cyber** dans une approche pluridisciplinaire croisant sciences mathématiques et informatiques avec sciences économiques, sociales et du comportement.

Sous l'impulsion d'**Airbus** et de l'**ANSSI**, l'IRT SystemX anime depuis novembre 2015 un groupe de travail sur « La maîtrise du risque cyber sur l'ensemble de la chaîne de sa valeur et son transfert vers l'assurance ». Il réunit des spécialistes de l'assurance et de la réassurance, des courtiers, des juristes, des actuaires, des industriels (risk managers), des experts de l'OCDE sous l'égide de la fédération française de l'Assurance (FFA), de l'association française de la réassurance (APREF), de *The Federation of European Risk Management Associations* (FERMA) et de l'association française des professionnels de la gestion des risques et des assurances (AMRAE).

Un **premier rapport de recherche[22]** a été rédigé et publié fin juillet 2016 (en français et en anglais). Le **deuxième cycle de séminaires** en 2017 sur la thématique de la **valorisation des biens intangibles** donnera lieu à la publication imminente d'un nouveau document.

Pour clore, cette première phase de travaux, nous proposons **un troisième cycle de séminaires**, qui **alterne réunions fermées**, **réunions en plénière** et **réunions en comités professionnels** courtiers, assureurs et réassureurs selon le calendrier en annexe. L'objet de ce séminaire est de réaliser **un exercice cyber s'appliquant à la filière aéronautique et de défense** selon une démarche proche de celle développée par l'Université de Cambridge ou des exercices cyber nationaux et internationaux (Piranet, Cyber Europe, Cyber Storm…).

L'exercice à trois objectifs : comprendre quelle est **l'ampleur de ces scénarios du point de vue du risque manager** d'un point de vue technique et métier, de les qualifier et les quantifier financièrement ; **étudier la réponse du marché de l'assurance** cyber (courtiers, assureurs, réassureurs) en termes de couverture du risque pour tous les acteurs de la filière (depuis les ETI jusqu'aux grands groupes) et **d'identifier les domaines assurables et non assurables** qui laisseront à la charge de la filière des risques non assurables résiduels pour lesquels elle doit s'organiser.

Les experts d'Airbus Group, **M. Philippe Cotelle** (Insurance and Risk Management), **Mme Bénédicte Suzan** (R&T and Innovation Coordination) avec l'appui de **M. Philippe Wolf** (Chef du projet EIC) conduiront ces réunions pour en exploiter les résultats. Ces échanges resteront confidentiels.

Dans l'attente de vous rencontrer, je vous prie d'agréer, Madame, Monsieur, l'assurance de ma sincère considération.

Philippe WOLF 

[21] Voir http://www.irt-systemx.fr/project/eic/
[22] Voir http://www.irt-systemx.fr/publications/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/

Annexe 4 – L'IRT SystemX

SystemX est l'un des huit instituts de recherche technologique qui ont été créés par le gouvernement pour renforcer l'attractivité du territoire.

« Un Institut de Recherche Technologique (IRT) est un institut thématique interdisciplinaire qui développe des filières économiques liées à son domaine au travers d'un partenariat stratégique public-privé équilibré. Pour cela, il pilote des programmes de recherche couplés à des plateformes technologiques, effectue des travaux de recherche et de développement au meilleur niveau international, contribue à l'ingénierie des formations initiales et continues (formation professionnelle qualifiante et/ou diplômante) ; et veille à la valorisation des résultats obtenus. »

Lancé en 2012, SystemX, unique Institut de Recherche Technologique (IRT) dédié à l'ingénierie numérique des systèmes du futur, répond aux défis scientifiques et technologiques de l'industrie et des territoires au moyen d'une innovation flexible, ouverte et collective.

Le fonctionnement de l'institut repose sur deux aspects fondamentaux :

- La colocalisation de ses talents. L'institut réunit au sein d'un même lieu tous les partenaires des projets, permettant ainsi de créer un véritable creuset d'interactions entre acteurs de la recherche publique et industrielle.
- La mutualisation des compétences et des plateformes. L'IRT SystemX consolide des plateformes technologiques grâce à la mise en commun de composants et d'infrastructures issus des projets de recherche, et développe des expertises, au service de ses partenaires publics et privés.

L'ambition est de développer des applications orientées marché et usages pour aider les industriels dans la transformation numérique de leur entreprise et leurs produits. Donc de répondre aux défis que rencontrent les industriels dans les phases de conception, de modélisation, de simulation et d'expérimentation des innovations futures qui intègrent de plus en plus de numérique au travers de quatre programmes :

- L'ingénierie systèmes : Développer des méthodes, des processus et des outils logiciels d'ingénierie collaborative pour les systèmes complexes, dans le contexte de l'entreprise étendue, tout en s'appuyant sur le potentiel des technologies numériques.
- Le transport autonome : Développer de nouvelles architectures sécurisées et sûres pour les véhicules et systèmes de transport autonomes, intégrant les nouveaux usages, les systèmes embarqués critiques, l'évolution des infrastructures et leurs interactions.
- L'Internet de confiance : Développer les algorithmes, les protocoles et les architectures sur lesquels reposeront les infrastructures numériques de demain, socle de la transformation numérique.
- Les territoires intelligents : Développer des outils d'aide à la décision pour l'optimisation et la planification opérationnelle de l'évolution des territoires, en s'appuyant sur la collecte et l'analyse des données.

Une convention entre l'IRT SystemX, l'ANSSI et Airbus Group couvre des actions de recherche en relation avec la protection et la défense des systèmes d'information. Ces travaux concernent les interactions entre les hommes et les techniques en cybersécurité dans leurs dimensions économiques et réglementaires. Ils visent à promouvoir les usages de confiance dans l'environnement numérique.

Les travaux de recherche de l'IRT sont validés par l'ANR (l'Agence nationale pour la recherche).

Annexe 5 – Le projet EIC

EIC : Environnement pour l'Interopérabilité et l'Intégration en Cybersécurité. Début des travaux, le 2 février 2015. Le programme de recherche est établi pour 5 ans. Le montant global du projet de recherche est estimé à 10M€, 12 ETP (montée en puissance prévue), 6 partenaires industriels à ce jour (Airbus Group, Bertin, Engie, Gemalto, Prove&Run, Thalès), des partenaires académiques (UTT de Troyes, IMT – Mines Télécom et CEA).

La protection des systèmes d'information et des données qu'ils véhiculent nécessite des arbitrages complexes entre la facilité d'usage, le coût de la sécurité, de la sûreté de fonctionnement et du respect d'un droit numérique en évolution constante afin d'offrir les conditions nécessaires à leur déploiement sur un marché ouvert pour créer rapidement de la valeur et réunir les conditions de la prospérité économique.

Plateforme CHESS : *Cybersecurity Hardening Environment for Systems of Systems* sur un financement de l'ANSSI à hauteur de1M€ sur 5 ans.

Dans ses 4 premières taches de recherche appliquée, le projet EIC met en œuvre la plateforme CHESS expérimentale et technique cyber afin évaluer le couplage de technologies de cybersécurité à travers des cas d'usage innovants dans le domaine des *SmartGrids*, de l'Usine du Futur, du Transport Connecté et Autonome et des nouveaux services de l'Internet des Objets.

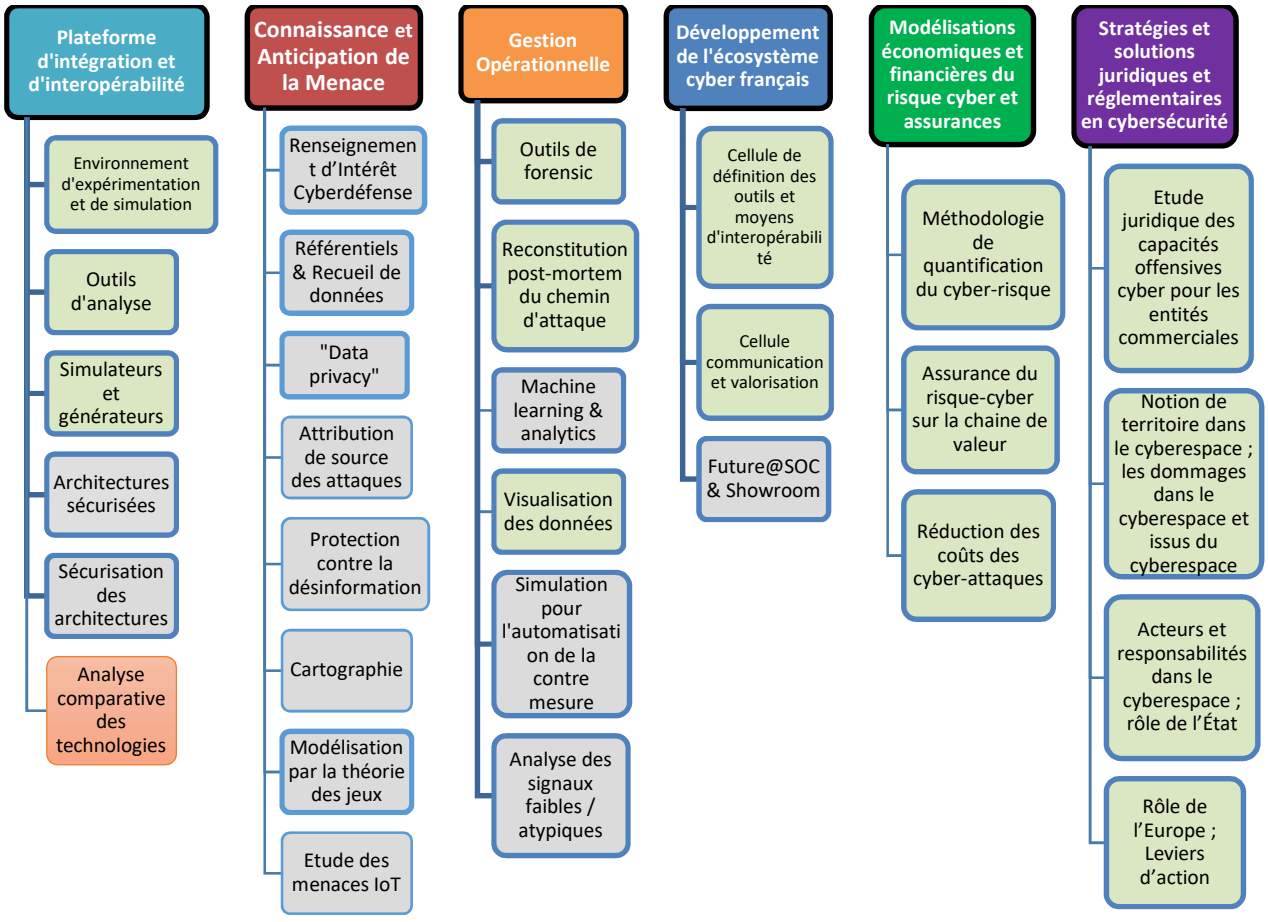


Figure 28 - décomposition du programme de recherche EIC en tâches et sous-tâches

Airbus finance depuis le 1er septembre 2015, les tâches 5 et 6 d'EIC qui viennent en appui des tâches 1 à 4 pour accompagner le développement des cas d'usage et permettre l'insertion de ces nouvelles technologies après leur

développement sur le marché. L'ANSSI finance également et, est directement partie prenante dans la définition des thèmes et la conduite de la recherche. Le financement de T5 et de T6 est ouvert à d'autres partenaires privés.

T5 et T6 traitent conjointement et de façon cohérente avec tâches 1 à 4 d'EIC des composantes économique/économétrique, financière, assurantielle et juridique du risque cyber.

Ces deux thèmes de recherche sont menés dans le cadre d'un Partenariat Public Privé faisant également appel à des acteurs extérieurs dont les compétences et la validation sont nécessaires et indispensables a priori.

T5.1 produit des travaux novateurs de modélisation économétrique afin de proposer une quantification du risque cyber et un mode de représentation afin de permettre aux responsables et au management de prioriser les investissements cyber et ensuite de réduire le risque (mitiger).

T5.2 traite des conditions nécessaires pour connaître, gérer et maitriser le risque cyber pour ensuite le transférer vers l'assurance. L'objectif étant de lever les verrous qui freinent aujourd'hui la compréhension risque cyber au sein des organisations et celles qui bloquent le développement du marché assurantiel de la cybersécurité. L'objectif de T5.2 est de pointer les obstacles et de produire des recommandations pour les lever dans un temps court au travers d'un plan d'action en fonction des calendriers législatifs et réglementaires en cours (nationaux et internationaux). 2017, publication du premier rapport de recherche sur les conditions du transfert du risque cyber d'une organisation vers le marché. 2018, publication du second rapport de recherche sur la valorisation des données intangibles en vue de leur transfert vers le marché de l'assurance. 2018, troisième séminaire de recherche sur le transfert du risque cyber sur la chaine de la valeur de la chaine d'approvisionnement de l'aéronautique et de défense.

Les travaux juridiques et réglementaires de T6 permettent à EIC d'introduire la sécurité juridique by design afin que les produits de la recherche appliquée et de l'innovation soient directement et dès le début encadrés et promus par un droit efficace pour les industriels sur le marché intérieur européen, mais aussi à l'extérieur (créateur de richesse et de croissance).

Annexe 6 – Les participants

Nous avons consulté des organismes acteurs du sujet à travers des personnes qualifiées, recommandées et invitées à participer aux travaux de réflexion durant la seconde année de notre programme de recherche. Cette liste n'est pas exhaustive.

Assureurs AIG AXA Entreprise ; Groupama ; Liberty Mutuel; Les Lloyds.	**Réassureurs** Libertyglobalgroup Munich-re France Partner-re SCOR SIRE Swiss-re
Courtiers Marsh GRAS SAVOYE NEOTECH - LSN SIACI Saint Honoré Clever Courtage	
Associations professionnelles APREF – Sous-Commission cyber FERMA – AMRAE FFA – GT cyber Institut des actuaires	
Cabinet de juristes KGA-Avocats	
Cabinet experts judiciaires ICA-ICSI	
Industriels, PME Airbus, Safran, Thales LINEON LATECOERE ERAMET	
Organisations internationales OCDE	**Ministère de l'Économie, de l'Industrie et du Numérique** ACPR – Banque de France
SGDSN / ANSSI	
IRT SystemX	

Annexe 7 – Le scénario Skyfleet rédigé

Timeline du scénario

Le 1 novembre 2018, une faille impactant le standard de communication des systèmes de gestion numérique d'entreprises connectées (ERP) gérant les commandes, factures, chaines d'assemblage est exploitée sur un 50% des fournisseurs du secteur aéronautique européen (uniquement). Les fournisseurs cessent brutalement de fonctionner, l'attaque affichant sur les terminaux utilisateurs des messages de blocage demandant une rançon de 250 000€. Les entreprises concernées ne peuvent plus traiter les commandes des clients, gérer leurs stocks et faire fonctionner leurs chaines d'assemblage.

Plusieurs entreprises tenteront de payer la rançon (demandée en monnaie cryptée pour ne pas être tracée) pour se rendre compte que les attaquants n'ont pas réellement prévu de solution de déblocage, leurs objectifs n'étaient pas monétaire mais de nuire aux entreprise concernées.

Parmi les entreprises victimes de cette attaque :

- **70%** réussissent à relancer leur ERP sous **1 semaine** grâce à une bonne utilisation de leurs sauvegardes (appelée "Entreprise de type A") (restauration au samedi précédent, dans la plupart des cas).
- **20%** restaurent leur ERP à **J - 1 mois**, perdant les informations de configuration de production, commandes, factures, stocks sur la période manquante. Toutefois certaines informations papiers restent disponibles. ("Entreprise de type B").
- **20%** ne parviennent pas à restaurer leur ERP et perdent de ce fait l'ensemble des informations de l'ERP à compter du 1er novembre. Seule la réinstallation de zéro du système est possible. Toutefois, certaines informations papiers restent disponibles. (Entreprise de type C).

Conséquences

Entreprise de type A : 1 semaine d'arrêt de production.

Entreprise de type B : 15 jours d'arrêt de production, 20% de baisse de rendement de production pendant 1 mois. Remise en question de la certification de(s) avion au niveau Avionneur (POA) par l'agence de certification (EASA), augmentation des couts de production pour l'entreprise fournisseur de 10%.*à etayer revalider/ cause-conséquences.*

Entreprise de type C : Perte du POA par l'EASA coté Avionneur, retour de la capacité de production sous 6 mois.

Le secteur aéronautique européen est porté par le constructeur "Skyfleet", et son modèle phare le "Skyfleet S410". La flotte de ce modèle se compose de **2560 avions** moyen-courrier en service dans le monde. **1000 avions** sont en commande de par le monde à cette date. A titre indicatif, le prix moyen d'un Skyfleet S410 est de **100M€**.

La production des avions est directement impactée à partir du mois de décembre 2018 se traduisant par une baisse des cadences de l'ordre **de 10% sur 3 mois**. Ce qui représente une impossibilité à livrer une 20aine d'avions sur la période.

Après 1 semaine, les investigations concluent que les attaques n'auraient pas pu avoir d'impact si les systèmes ERP avaient été configurés dans les règles de l'art (comme observé chez d'autres fournisseurs non atteint).

Pour information, une grande majorité (80%) des entreprises touchées avaient externalisé l'installation et l'exploitation de leur ERP à la société "SG3".

Détails techniques du scénario :

L'attaquant utilise une faille de configuration (couple user/mot de passe par défaut) pourtant imposé en changement par l'éditeur afin d'envoyer des instructions protocolaires à l'ERP de niveau administrateur.

En utilisant cet accès, il active une fonction native des ERP permettant de chiffrer les données de celui-ci, puis supprime la clé de déchiffrement à distance via les mêmes commandes. Cette fonction est utilisée habituellement afin d'interdire l'accès aux données de production par un administrateur).

La mise en place de l'attaque prend **1 mois**, le temps d'effectuer le chiffrement des données et de supprimer la clé de déchiffrement.

La coupure de l'accès aux données de production est réalisée en supprimant les clés de chiffrement du système.

Scénario alternatif :

La coupure de l'accès aux données de l'entreprise est toujours réalisée en supprimant l'accès aux clés de chiffrement, celles-ci étant elles-mêmes chiffrées par un programme tiers installé par l'attaquant et résidant en mémoire (attaque de type fileless). La suppression de cet accès est réalisé par un reboot du système qui supprime ainsi le seul moyen d'accès aux données qui se retrouve ainsi prises en otage.

Si ce scénario est retenu, les conséquences sont plus importantes car la répartition des entreprises victimes sera alors :

- Entreprises de type B : 80%
- Entreprises de type C : 20%

Le résultat final des investigations parvient à décrire précisément comment l'attaque a été menée. Cependant, elle ne permet malheureusement pas d'attribuer celle-ci à une organisation identifiée. Toutefois, des motivations géopolitiques et économiques sont soupçonnées aux regards des capacités technologiques mises en œuvre, de la couverture géographique limitée et de l'impossibilité de communiquer avec l'attaquant pour payer une éventuelle rançon.

Impacts sur le constructeur, les *suppliers* de rang 1 et le reste de la *supply chain*.

La quantification du scénario prendra en compte les capacités de résilience de filière aéronautique.

Information quantitatives :

- *Supply Chain* : 15 000 entreprises dont 2 500 avec des systèmes ERP connectés à Internet
  - PME – CA < 50M€ : 68% ;
  - ETI – CA < 250M€ : 30% ;

- GE (Grande entreprise) : 2% ;
- Chiffre d'affaire de l'avionneur "Skyfleet" : 40m€
- Part du chiffre d'affaire représentée par le modèle d'avion concerné "S410" : 6m€
- S€ par an

Nationalité du constructeur Skyfleet : française.

Répartition Géographique des fournisseurs:

- Europe : 66%
  - France : 47% ;
  - Allemagne : 25% ;
  - Angleterre : 20% :
  - Autres : 8%.
- US : 25%
- Autres : 9%

Méthodologie/Prochaines étapes

2 approches pour la quantification : partir de l'avion produit ou du CA.

20 avions non produits, marge brute 20% avec décote appliquée pour décalage de production.

En PD/BI : 260M€ pour le Prime, conséquences pour les acteurs de la supply chain à déterminer (essentiellement les T1)

Définir le nombre d'entreprise touchée par l'attaque et les répartir dans les 3 types A, B et C.

Pénalités contractuelles (clients pour retard de livraison 15%/2 (négocié) de pénalités avec un total de 50M€ par mois pendant 3 mois)

Annexe 8 – Cyberguerre ?

Rédacteur: Philippe Wolf

Une clause d'exclusion ?

« *Zurich Insurance Group* a refusé de régler 100 millions de dollars de dommages-intérêts suite à la réclamation d'assurance de Mondelez, géant états-unien de l'alimentation, relativement à une cyberattaque de NotPetya. Ce refus a poussé Mondelez à intenter une action en justice contre son assureur devant le tribunal du comté de Cook en Illinois pour refus de paiement suite à la cyberattaque de 2017 [Le siège de Mondelez est dans l'Illinois]. »[23]

Cette bataille juridique à venir sera, bien sûr, suivie attentivement par les acteurs de l'assurance.

Les articles 20 et 21 de la Loi n° 67-522 du 3 Juillet 1967 sur les Assurances Maritimes écartent, sauf convention contraire :

« Article 20 - L'assureur ne couvre pas les risques :a) **de guerre civile ou étrangère**, de mines et tous engins de guerre ; b) de piraterie ; c) de capture, prise ou détention par tous gouvernements ou autorités quelconques ; d) d'émeutes, de mouvements populaires, de grèves et de lock-out, d'actes de sabotage ou de terrorisme ; e) des dommages causés par l'objet assuré à d'autres biens ou personnes, sauf ce qui est dit à l'article 43 ; f) des sinistres dus aux effets directs ou indirects d'explosion, de dégagement de chaleur, d'irradiation provenant de transmutations de noyaux d'atomes ou de la radioactivité, ainsi que des sinistres dus aux effets de radiation provoqués par l'accélération artificielle des particules.

Article 21 - Lorsqu'il n'est pas possible d'établir si le sinistre a pour origine un risque de guerre ou un risque de mer, il est réputé résulter d'un événement de mer »

Le code des assurances précise dans son Article L121-8 (Version en vigueur au 21 juillet 1976) :

« L'assureur ne répond pas, **sauf convention contraire**, des pertes et dommages occasionnés soit par la guerre étrangère, soit par la guerre civile, soit par des émeutes ou par des mouvements populaires.

Lorsque ces risques ne sont pas couverts par le contrat, **l'assuré doit prouver que le sinistre résulte d'un fait autre que le fait de guerre étrangère** ; **il appartient à l'assureur de prouver** que le sinistre résulte de la guerre civile, d'émeutes ou de mouvements populaires. »[24]

La réassurance peut être mise à contribution : « Par ailleurs, **l'état se désengage** et les assurances ou réassurances des risques de guerre sont pris en charge par la CCR (Caisse Centrale de Réassurance) avec la garantie de l'état (L 431-4 du Code des assurances) » [25].

Les analystes constatent : « Les risques de guerre sont les seuls aujourd'hui légalement exclus à raison de leur caractère inassurable. Il faut distinguer selon que sont en cause les assurances de choses et de personnes. En réalité aujourd'hui, n'est expressément exclu que le risque de guerre dans les assurances de dommages de biens. L'article L121-8 al1 […] édicte une exclusion légale en des termes non impératifs puisque cette exclusion vaut sauf convention

[23] Voir https://www.developpez.com/actu/244586/Une-compagnie-d-assurance-dit-que-NotPetya-est-un-acte-de-guerre-et-refuse-de-payer-ce-qui-pourrait-creer-un-mechant-nouveau-precedent/

[24] https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006073984&idArticle=LEGIARTI000006792318&dateTexte=&categorieLien=cid

[25] Code des assurances, Version consolidée au 8 février 2019 https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006073984

contraire. Donc **il n'est pas interdit de couvrir le dommage de guerre**. Le régime de l'exclusion diffère selon les dommages par le fait de guerre étrangère ou par une guerre civile, émeute, mouvement populaire. Le texte dit en effet, lorsque ces risques ne sont pas couverts. »[26]

Pour toute attaque informatique, il faudra répondre aux questions suivantes dans une obscurité numérique propice aux dissimulations : qui m'attaque ?, quel dommage ?, comment ?, pourquoi ?[27].

Il convient alors de s'interroger sur le concept de cyberguerre et sur la qualification des attaques massives contre des systèmes cyber-physiques dont l'opération *Olympic Games* (Stuxnet) découverte en 2010 marque probablement la première manifestation médiatisée. Le débat est ouvert. Les quelques éléments qui suivent ne font que souligner sa difficulté.

Une définition de la cyber-guerre ?

Constat principal, *« cyberwar is storystelling »*[28]… La cyberguerre fait l'objet depuis quelques années de nombreuses publications, études, colloques, discours et même ou surtout fictions, sous toutes ses formes (dans le film *Skyfall* de 2012, l'ennemi de James Bond est un ancien agent du MI6 devenu cyber-terroriste).

La cyberguerre, les pays « anglo-saxons » s'y intéressent depuis longtemps : dès 1993 en effet, les États-Unis — le *Department of Defense* (DOD) - Joint Chiefs of Staff — définissent le concept de guerre de l'information (*information warfare*[29]) puis Martin C. Libicki (*Institute for national strategic studies*, 1995), distingue et définit sept domaines dans la guerre de l'information[30]. C'est en juillet 2002 que le président George W. Bush a signé une directive secrète de Sécurité nationale qui autoriserait l'usage offensive d'armes cybernétiques (HSPD 16; Homeland Security Presidential Directive 16) et dont les révélations d'E. Snowden décriront l'ampleur.

La France, après beaucoup d'autres pays, a rendu publique en 2018 sa doctrine de lutte informatique offensive[31] tout en prévenant l'usage de ces techniques par des acteurs privés[32]. Mais l'informatique est aujourd'hui duale.

Le document public français précise : « La **lutte informatique offensive à des fins militaires** (LIO) recouvre l'ensemble des actions entreprises dans le cyberespace, conduites de façon autonome ou en combinaison des moyens militaires conventionnels. L'arme cyber vise, dans le strict respect des règles internationales, à produire des effets à l'encontre d'un système adverse pour en altérer la disponibilité ou la confidentialité des données. »

Il est à noter que la Russie s'active à l'ONU depuis 1998 pour promouvoir des cyber-lois internationales, notamment à travers le think-tank des États-Unis *EastWest Institute*[33]. Leur définition était proche de la définition française : « La

---

[26] http://www.cours-de-droit.net/les-exclusions-legales-des-risques-dans-les-contrats-d-assurances-a126584520

[27] *Cyber-conflits, quelques clés de compréhension*, Philippe Wolf et Luc Vallée, 2011, https://www.ssi.gouv.fr/uploads/IMG/pdf/Cyber_conflits_quelques_cles_de_comprehension.pdf

[28] Martin C. Libicki, "Cyberwar is storytelling" in *Crisis and Escalation in Cyberspace*, http://www.rand.org/pubs/monographs/MG1215.html

[29] La typologie est détaillée dans le livre d'E. Waltz, *Information Warfare-Principles and Operations*, Artech House Publishers, 1998.

[30] Martin C. Libicki, "What Is Information Warfare?", *Strategic Forum* Number 28, May 1995, voir http://www.dodccrp.org/files/Libicki_What_Is.pdf

[31] Dans *Éléments publics de doctrine militaire de lutte informatique* offensive https://www.defense.gouv.fr/content/download/551555/9394645/El%C3%A9ments%20publics%20de%20doctrine%20militaire%20de%20lutte%20informatique%20OFFENSIVE.pdf

[32] Karine Bannelier, Théodore Christakis, "Prévention des attaques informatiques et protection : qui doit faire quoi?", « Construire la paix et la sécurité internationales de la société numérique », Agence Nationale de Sécurité des Systèmes de l'Information/Ministère des affaires étrangères, Paris, UNESCO, 6-7 avril 2017.

cyberguerre **est un état d'escalade d'un cyber conflit** entre les États où les cyberattaques sont menées par des acteurs étatiques contre les cyber infrastructures **dans le cadre d'une campagne militaire** – (i) **déclarée**: déclarée formellement par une autorité de l'une des parties. – (II) **de facto: avec l'absence de déclaration** ».[34]

Malgré cela, la différence, facile à comprendre, entre sécurité des systèmes d'information — terme introduit en France en 1986 — et sécurité de l'information est, avec d'autres considérations simplement géopolitiques, un des points d'achoppement de toutes les négociations internationales dont il serait fastidieux de faire l'énumération : ONU, IUT, OCDE, etc. Ainsi, la cinquième édition du groupe d'experts gouvernementaux des Nations Unies (GGE) — chargée d'élaborer une « compréhension commune » de la manière dont les États devraient se comporter dans le cyberespace — a échoué mi 2017[35]. Le droit moderne de la guerre (*jus in bello* et *jus ad bellum*) depuis les conventions de La Haye jusqu'aux conférences de Genève a mis des dizaines d'années à s'établir. L'établissement **d'un droit de la cyberguerre** devra probablement s'établir avec une urgence plus grande.

	Conflit : Stuxnet USA	Conflit : Georgie Russie
INTERNATIONAL CYBER SECURITY LAW		
RULE 1 – Sovereignty		
RULE 2 – Jurisdiction		
RULE 3 – Jurisdiction of Flag States and States of Registration		
RULE 4 – Sovereign Immunity and Inviolability		
RULE 5 – Control of Cyber Infrastructure		
RULE 6 – Legal Responsibility of States		
RULE 7 – Cyber Operations Launched from Governmental Cyber Infrastructure		
RULE 8 – Cyber Operations Routed Through a State		
RULE 9 – Countermeasures		
RULE 10 – Prohibition of Threat or Use of Force		
RULE 11 – Definition of Use of Force		
RULE 12 – Definition of Threat of Force		
RULE 13 – Self-Defence Against Armed Attack		
RULE 14 – Necessity and Proportionality		
RULE 15 – Imminence and Immediacy		
RULE 16 – Collective Self-Defence		
RULE 17 – Reporting Measures of Self-Defence		
RULE 18 – United Nations Security Council		
RULE 19 – Regional Organisations		

Figure 29 - analyse succincte de conflits cyber avec le manuel de Tallinn

Le document de référence le plus complet à ce jour est le manuel dit de Tallinn[36], un guide en anglais rédigé par un groupe d'experts mandatés par l'OTAN, qui propose une transposition du droit international aux conflits cyber. Il est cependant aujourd'hui patent que des opérations aux effets de bord mesurables (voir ci-après) n'en respectent pas les règles, à l'image d'une analyse partielle visualisée ci-dessus (en rose les non-respects des règles).

---

[33] Russia-U.S. Bilateral on Cybersecurity: Critical Terminology Foundations, avril 2011, https://www.eastwest.ngo/idea/russia-us-bilateral-cybersecurity-critical-terminology-foundations

[34] Traduction de : "Cyber War is an escalated state of cyber conflict between or among states in which cyber attacks are carried out by state actors against cyber infrastructure as part of a military campaign – (i) Declared: that is formally declared by an authority of one of the parties. – (ii) De Facto: with the absence of a declaration."

[35] Voir https://www.lawfareblog.com/un-gge-failed-international-law-cyberspace-doomed-well

[36] Disponible ici : http://csef.ru/media/articles/3990/3990.pdf

De Wannacry à NotPetya : 2017

Des fuites récentes, provenant de sources non identifiées fin 2017[37], et dont la diffusion publique partielle est assurée par le site Wikileaks[38] ont généré, depuis mai 2017, la création de pièges dont la fonction principale n'est plus le chantage ou rançonnage[39] mais la destruction de données numériques.

Technique d'attaque courante de la cybercriminalité, le rançongiciel ou ransomware consiste en l'envoi à la victime d'un logiciel malveillant qui chiffre l'ensemble de ses données et lui demande une rançon en échange du mot de passe de déchiffrement.

Ainsi le code malveillant auto-réplicant Wannacry (WannaCrypt, WanaCrypt0r), maquillé en rançongiciel dont il prend les apparences, exploite une faille de sécurité informatique de type 0-day affectant, potentiellement, l'ensemble des systèmes Windows non mis à jour antérieurs à la version 10. Ce rançongiciel se caractérise par sa fréquence d'attaque qui a été d'au moins une tentative par seconde et de 226 800 adresses Internet affectées à son point fort. Des entreprises victimes ont communiqué, dont Renault en France.

0-day : catégorie particulière de codes d'exploitation qui cible des vulnérabilités qui ne sont pas encore publiquement annoncées par l'éditeur, le constructeur ou un chercheur en sécurité) puisque la correction n'a été rendue disponible qu'après les premiers dégâts.

Ce logiciel ne semblait pas être développé à l'état de l'art (une hypothèse plausible semblerait alors être une diffusion prématurée ou accidentelle). Un de ses mécanismes particuliers est original. Il s'agit d'une fonction de coupe-circuit (*killswitch*) qui a beaucoup fait s'interroger les spécialistes : c'est le non enregistrement d'un domaine sur Internet qui entraînait l'arrêt de la propagation du malware. Ce mécanisme a été supprimé dans des variantes plus récentes.

NotPetya qui doit son nom à la ressemblance avec le code malveillant Petya, découvert initialement en Ukraine en mars 2016, apparait le 27 juin 2017 et touche l'ensemble de la gamme Windows en exploitant une vulnérabilité dont le correctif, publié en mars, n'a pas été appliqué dans certains environnements productifs (comme Saint-Gobain, Auchan et la SNCF en France). Il intègre deux outils de piratage volés à la NSA. Contrairement aux habituels ennemis russes ou chinois, c'est la Corée du Nord[40] qui a été initialement désignée comme source de ces nouveaux logiciels destructeurs. En attendant, peut-être, de nouveaux éléments qu'il faudra apprécier avec prudence, la désinformation étant l'alliée de tout acte malveillant dans le cyberespace.

[37] Une source possible est présentée ainsi par Wikipedia : *The Shadow Brokers (littéralement « les courtiers de l'ombre ») est un groupe de hackers connu pour avoir dévoilé en 2016 des outils d'espionnages, entre autres, de l'Equation Group, une unité de hackers soupçonnée d'être lié à la National Security Agency (NSA)*.

[38] https://wikileaks.org/vault7/

[39] Philippe Laurier, Les cyberattaques et leurs préjudices sur les entreprises : quantification et qualification, 19 septembre 2017, http://www.irt-systemx.fr/wp-content/uploads/2017/10/ISX-IC-Cyber-Risque.pdf

[40] Comme l'affirmait, par exemple, le Britain's National Cyber Security Centre (NCSC) http://www.bbc.com/news/technology-40297493

Et maintenant ?

Nous sommes entrés dans l'ère de l'*Internet of Everything*. On nous annonce 50 milliards d'objets connectés en 2020 et 1000 milliards en 2035 soit près de 200 dispositifs électroniques par personne, en considérant que les internautes constitueront plus de la moitié de l'humanité (c'est le cas depuis 2017). 500 millions d'applications offriront des services à partir de ces capteurs. Cela ouvre un terrain de jeu immense pour les attaques ciblées ou non. « L'Internet est un marécage », affirme Louis Pouzin, l'un de ses pionniers français. Il devient dès lors facile d'imaginer des catastrophes numériques qu'il faudra prévenir demain par une meilleure résilience.

Un article étasunien récent, faisant suite à l'affaire Mondelez, appelle à un dialogue entre gouvernements et assureurs :

« En fin de compte, l'ampleur même du défi posé par le cyber-risque signifie que les gouvernements et les assureurs doivent travailler en étroite collaboration. Il ne faut pas laisser aux entreprises individuelles, ni même aux tribunaux, le soin de déterminer le parrainage de l'Etat pour les cyberattaques ou de forcer Zurich et d'autres compagnies d'assurance à supporter l'essentiel de la cyber agression soutenue par l'Etat. Les assureurs ont besoin d'être à l'abri des cyberattaques les plus graves, quelle que soit leur origine, sous la forme d'un filet de sécurité gouvernemental en cas de cyber-risque catastrophique, semblable au programme d'assurance contre le risque terroriste du ministère du Trésor, qui prévoit la réassurance des attaques terroristes massives. Un tel filet de sécurité ne peut se faire sans exigences et conditions préalables, de sorte que les gouvernements et les assureurs doivent collaborer pour trouver un équilibre réaliste entre leurs responsabilités.

L'affaire Mondelez-Zurich souligne l'urgence d'une action gouvernementale pour éliminer ces obstacles et faire face aux risques qui entravent un marché de la cyber assurance plus robuste. Cela sera essentiel pour libérer le potentiel de l'assurance de diminuer et de canaliser le risque, un rôle qui s'est avéré vital pour la gestion des menaces traditionnelles. »[41]

[41] Traduction par DeepL de la conclusion de l'article : https://www.lawfareblog.com/moment-truth-cyber-insurance

IX. Translation of Summary Chapters

NB: The reference document is in French. Only Summary Chapters I to IV are translated into English.

THE CONTROL OF CYBER RISK THROUGHOUT THE VALUE CHAIN AND ITS TRANSFER TO INSURANCE
Cyber scenario applicable to the aeronautics industry
Market response

RESULTS OF RESEARCH: a summary

Year 3: Seminar February 2018 - February 2019

REPORT PREPARED BY

Philippe Cotelle Insurance Risk Manager in charge of Cyber Risk for AIRBUS	PhilippeWolf Project Manager EIC IRT SYSTEMX	Bénédicte Suzan Rédacteur principal R&T Innovation Cooperation AIRBUS Defense and Space
Groupe de travail des coutriers Jean-Laurent Santoni CleverCourtage	**GT Cyber FFA** Laurence Lemerle, AXA Christophe Delcamp, FFA	**Sous-Commission Cyber APREF** Virginie Wyka, PARTNER RE Sébastien Héon, SCOR

IN PARTNERSHIP WITH

FOR ANY INFORMATION CONCERNING THIS REPORT, YOU MAY CONTACT THE IRT SYSTEMX AT THE FOLLOWING COORDINATES: IRT SystemX, 8, avenue de la Vauve, CS 90070 - 91127 Palaiseau Cedex

Website: www.irt-systemx.fr ; E-mail: philippe.wolf[at]irt-systemx.fr

X. Presentation of the work

As part of its EIC[42] (Environment for Interoperability and Integration in Cybersecurity) project, IRT SystemX is conducting research on **cyber risk management** in a multidisciplinary approach that combines mathematical and computer sciences with economic, social and behavioural sciences.

Under the leadership of the Chief Security Officer of **AIRBUS** and the Director General of **ANSSI** (Agence nationale de la sécurité des systèmes d'information), IRT SystemX has been leading a working group since November 2015 on "Managing cyber risk throughout the value chain and its transfer to insurance". It brings together insurance and reinsurance specialists, brokers, lawyers, actuaries, industrialists (Insurance Risk Managers), OECD experts, under the aegis of the Fédération Française de l'Assurance (FFA), the Association française des professionnels de la réassurance en France (APREF), the Association française des professionnels de la gestion des risques et des assurances (AMRAE) and The Federation of European Risk Management Associations (FERMA).

A **first research report**[43] was written and published at the end of July 2016 (in French and English).

Year 1 of the research was organized between plenary meetings and preparatory meetings between each. The report and recommendations highlight the importance of conducting a financial quantification of cyber risk within the company, defining a common reference framework and language for the various stakeholders, establishing new communication rules between them (the issue of confidentiality has contributed to the implementation of the ACYMA[44] cyber-monitoring platform, in which the FFA is a partner for a better understanding of exposure and claims, the support to be provided to companies suffering losses) and developing a better knowledge of insurance coverage (see matrix). This question has since been taken up again in the framework of the report of the Lawyers' Club (better understanding and apprehending cyber coverage) [45] and in a form improved by the OECD[46]. The work also highlighted the weight of silent covers, or non-affirmative covers. A subject that the profession has been working on since then. Research work thus helps to build the branch that is currently developing. As for the lack of definition and legal qualification of the data, the law is developing less quickly than technology and its uses.

Some of these recommendations were included in the SGDSN Cyber Defence Strategy published in March 2018, including the privacy requirements for cyber-attacks[47].

[42] See http://www.irt-systemx.fr/project/eic/

[43] See http://www.irt-systemx.fr/publications/english-la-maitrise-du-risque-cyber-sur-lensemble-de-la-chaine-de-sa-valeur-et-son-transfert-vers-lassurance/

[44] https://www.cybermalveillance.gouv.fr/

[45] https://www.leclubdesjuristes.com/wp-content/uploads/2018/01/cdj_assurer-le-risque-cyber_janvier_2018_fr.pdf

[46] https://www.oecd.org/pensions/The-cyber-insurance-market-responding-to-a-risk-with-few-boundaries.pdf

[47] http://www.sgdsn.gouv.fr/evenement/revue-strategique-de-cyberdefense/

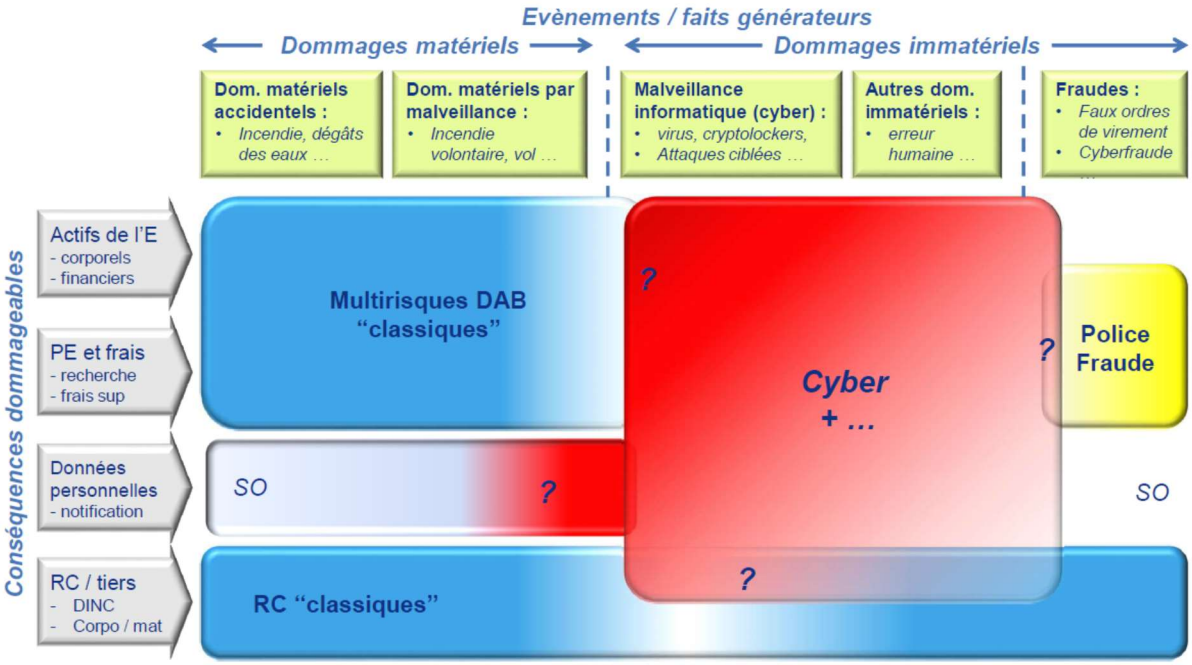


Figure 30 - Synthetic matrix Damage generating events / Guarantees

The **second cycle of seminars** in 2017 focused mainly on **the valuation of intangible data necessary to know, manage and control cyber risk and then eventually transfer it to insurance**. A **second research report** was published in January 2019[48]. This report[49] was written and published in French and English.

Year two of the research focused on an ambitious subject, the transfer of intangible property to insurance. Since then, other reports have addressed the subject on the valuation of companies' intangible assets. A subject for which it is still difficult to provide answers but which is strategic for the future of cyber risk governance.

A number of external stakeholders provided insights such as rating agencies, auditors, insurers and researchers to help understand how they contribute to the organization's valuation of cyber risk. The financial valuation of companies increasingly takes into account the intangible value of their data - the information assets. This is a real paradigm shift because 20 years ago, according to the OECD, 75% of the value of companies was tangible, today the figures are reversed. The valuation of the company is essentially constitutive of intangible assets. The latter are by definition more sensitive to cyber risk, such as data and reputation.

Rating agencies presented how cyber risk was part of their assessment of a company's risk quality, since if its valuation is at risk, this cyber risk may be an element taken into account. The answer is yes, under pressure from investors in particular, because they need this information that will allow them to take into account the investment decision over time. At the same time, the agencies have highlighted modelling problems. In this sense, the problems of insurers are similar to those of rating agencies. Lawyers were interviewed to understand what the impact on executives' exposure to cyber risk is: does this element expose them personally as a corporate officer? Researchers have also contributed to the question of whether it is possible to financially value these intangible assets and whether it is possible to associate a financial value with data

[48] Ibid.

[49] https://www.irt-systemx.fr/wp-content/uploads/2019/01/ISX-EIC-transfert-risque-an2.pdf

outside the scope of trademark and intellectual property. The study of court decisions has made it possible to give financial assessments in terms of intangible data loss. The evolution of accounting standards is an international negotiation issue - IFR 48 recently excluded intangible assets. A theoretical and intellectual basis for progress on these issues does not exist today, but work is ongoing.

The work carried out within the IRT SystemX should contribute to a better understanding of the challenges of cyber risk for VSEs and SMEs. This is a significant issue for startups whose value is their innovation and research. If this information is compromised, the value of the company is affected. The issue of protecting innovation and developing the increasingly digitalized economy of the future is a major one. In addition to the question of data valuation, there is now also the question of knowledge valuation: the problem of artificial intelligence, the ethics of algorithms, the liability of robots and the legal personality of embedded systems, the automotive industry and connected aircraft without pilots. Many questions are open.

Insurance and reinsurance companies note this lack of financial valuation of intangible assets.

The conclusions of this second year may have been less constructive in terms of deliverables on the response of the insurance market in its ability to insure intangible assets, but they have made it possible to launch discussions between insurers and reinsurers on the advisability or otherwise of indexed, parametric contracts.

The recommendations of the second year of the work call for the need for internal implementation of cyber risk governance and the ability to define the need for coverage internally - see also the work of FERMA[50] and that conducted with Insurance Europe[51]. The framework for companies' external communication on their exposure to cyber risk is becoming an important element.

The quantification of cyber risk also requires a standardized framework to compare the level of cyber maturity and governance of organizations with each other in their risk analyses and for the quantification of their scenarios. It is a question of agreeing to take into account the risk, remediation and vigilance phase in their assessments. Companies must be able to communicate on exposure status based on a common reference framework so that those involved in the valuation of companies can understand and compare one company with another in a reasonable way.

On the obligations and liability of managers under their D&O and cyber policies, the existing coverage is currently positive and it would be appropriate to maintain this status.

Regarding the financial assessment of an impact on intangible assets, progress needs to be made, but the trend is there, both by companies as rating agencies and their investors question them on how value is protected. For insurers, a new field is clearly opening up for the protection of intangible assets in an increasingly digitalized economy.

In the debates on the challenges of cyber insurance, access to data, the risk of accumulation, the problem of modelling, the problem of silent coverage have not been highlighted.

The **reflections of year 3** focused on **the design and implementation of a cyber exercise applicable to the aeronautics sector** according to an approach similar to that developed by the University of Cambridge or national and international cyber exercises (Piranet, Cyber Europe, Cyber Storm...). The objective was to reflect on the concept of Extended Enterprise and to question the fact that today, an organization must be

[50] https://www.ferma.eu/exclusive-ferma-eciia-cyber-risk-governance-report-available?type=advocacy

[51] https://www.insuranceeurope.eu/sites/default/files/attachments/Preparing%20for%20cyber%20insurance.pdf

able to assess cyber risk along its value chain and supply chain for which raising the level of maturity in cyber security is a strategic issue.

The starting point for our reflections was the initiative taken by BoostAerospace - Extended Enterprise (see Annex 1), the secure exchange platform for suppliers in the aeronautics industry who wish to set up Bronze, Silver, Gold technical cyber security standards adapted to the industry. The principle of such an approach is also shared by AMRAE, which believes that it is less for the regulator to impose high-level technical and governance standards for cyber security than for manufacturers who know their needs. In view of BoostAerospace's initiative to raise the level of investment in cyber security, there is a real opportunity to highlight the need for cyber coverage for the entire supply chain. It is indeed realistic to think that it will be possible to match technical standards to a need for coverage and to develop mirror coverage in the future. It is realistic to think that, in the medium term, Bronze, Silver or Gold subcontractors may as such communicate with insurers who would recognize these standards. Understanding what emerges, insurers would be in a better position to offer appropriate coverage.

The exercise as a whole assesses the resilience of the supply chain to cyber risk by showing the economic cost of a catastrophic scenario and comparing it to the financial amounts that are insured and reinsured.

The numerical estimates make it possible to present ANSSI with a first financial quantification of a disaster scenario affecting an industrial sector. They also enable final integrators in the aeronautics sector to better understand the sector's exposure to cyber risk, what are the impacts for tier 1 companies and subcontractors and thus highlight the size of an exhibition of which they may not have a clear knowledge. They provide brokers, insurers and reinsurers with a better understanding of the challenges of cyber resilience in the aviation industry.

The disaster scenario does not include the quantification of the financial consequences of the attack on the ordering aircraft manufacturer.

XI. Research approach

This report details the results of the research approach described below.

XI.1. Conduct of the research

The seminars were organised around the following calendar:

Seven preparatory meetings were necessary to draft the support scenario for the exercise with the knowledge of the aeronautics sector (Insurance Risk Managers of Airbus, Safran and Thales), cyber experts, experts from ANSSI, the Chief Information Security Officers of Airbus and BoostAerospace, in the presence of CISOs from BoostAerospace partner companies (the CISO of Latécoère, the CISO of ERAMET), the French Federation of Insurance (FFA), reinsurance and cyber security experts and a representative from Airbus General Procurement.

The qualified and quantified scenario was presented to the players in the insurance market: brokers, insurers and reinsurers at the opening session.

An alternation of plenary sessions and closed professional committees punctuated the research exercise for this year 3 so that each plenary session would allow the committees presenting their work to share their thoughts and conclusions.

The broker committee met once during the IRT SystemX seminar.

The insurance committee met twice during the IRT SystemX seminar. The conclusions were prepared within the framework of the FFA Cyber Working Group. Which has met internally with FFA on nearly 5 occasions. A survey was also conducted among the members of the Federation.

The reinsurance committee met once during the IRT SystemX seminar. The cyber sub-commission of the Association des Professionnels de la réassurance en France (APREF) met internally 3 times to answer the questions asked.

An additional meeting of the IRT SystemX seminar brought together the two working groups FFA and APREF, which had previously organised a joint meeting of their two working groups.

The seminar concluded with a final meeting during which brokers, insurers and reinsurers presented the main elements of their response to the scenario. The final meeting summarized the lessons learned and prepared the recommendations (see chapter IV.)

XI.2. Purpose of the exercise

The aim is to test the cyber risk scenario (see chapter V.) throughout the value chain, from suppliers to the final integrator in the aerospace industry.

Five main objectives are pursued:

1. Understand the magnitude of the scenario from the Insurance Risk Manager's point of view, qualify it and quantify it financially.
2. Study the response of the cyber insurance market (brokers - Chapter VI., insurers - Chapter VII., reinsurers - Chapter VIII.) in terms of risk coverage for all players in the sector: from ETIs (mid-cap companies) to large groups.
3. What insurance cover would be provided for this exercise?

4. How would reinsurers manage their accumulations?
5. Identify the insurable and non-insurable areas that will leave the industry with residual non-insurable risks for which it must organize itself.

XI.3. Conclusions of the exercise

Nota Bene:

Chapters VI, VII and VIII, describing the response of the cyber insurance market, are more technical. We have preferred to keep in this report all the factors studied and taken into account to the detriment of a more complete drafting. In particular, omissions (e.g. potential airline claims) are noted.

These results demonstrate the feasibility of a detailed analysis of a scenario that is intended to be realistic[52] and prefigure new methods that are still in the co-construction phases between all stakeholders.

[52] See, for example, https://www.zdnet.fr/actualites/50-000-entreprises-utilisent-un-logiciel-sap-vulnerable-39884273.htm

XII. Summary of research results

The work sought to quantify in the cyber-attack scenario chosen on the actors of the aeronautics supply chain what could be the impact ensured for the entire aeronautics industry. We do not have, at this stage, a credible figure on the economic impact - the aggregate direct and indirect economic costs that would come beyond this assured impact. Our estimate therefore represents only a portion of the real economic impact suffered by the sector.

In this scenario, in view of many assumptions that will be detailed later, the figures show a financial impact on the insurance contracts of the principal's subcontractors (without cost assessment for the latter) of around 400M euros. This amount corresponds to the mobilization of insurance contracts for 11% of the aircraft manufacturer's subcontractors. This amount does not take into account the consequences on the other economic sectors for which subcontractors also work.

In addition, reinsurance estimates that nearly 80% of the insured amount would actually be carried by reinsurance. It is financially able to respond to the disaster. However, if reinsurance were to pay such a claim at the industry level, according to an average premium estimated at €5,000 for the 1800 companies in the scenario for a total premium estimated at €9 million, the induced return period would be 46 years although such a scenario appears to have a much higher probability of occurrence (once every 46 years). The amount of premiums allocated to cyber risk therefore still seems insufficient to respond to major events.

This study shows that reinsurance has a real lever to effectively contribute to the development of the cyber insurance market since reinsurers are the ones who ultimately bear the risk of a catastrophic cyber scenario: the management of accumulation is, for them, a particularly important problem. Faced with cyber insurers who are online, it is the reinsurers who offer the ultimate financial means to provide the coverage that will be triggered by the policyholders.

Reinsurers have also particularly highlighted the problem of defining the event necessary to set up reinsurance contracts for systemic events. Since a cyber event is not limited in time, space, causes and targets can be varied, it is currently complicated to qualify it. They recommend working on a robust and recognized definition of the cyber catastrophic event. The analogy with the definition of a catastrophic natural event, where each hurricane, earthquake... is clearly identified allowing the application of covers in an undeniable way is not effective for the cyber.

Reinsurers and insurers also point to the risk of clashes between the different reinsurance solutions, which leads to a difficult to identify and therefore uncontrolled accumulation of cyber claims carried by reinsurance. Between the various Quota-Share and Excess treaties by risk as well as by type of treaty, whether they are specific cyber reinsurance treaties or more traditional guarantees, the management of exposures and accumulations is a real problem for reinsurance. Clarification and better identification of these mechanisms for reversing cyber exposure under the treaties is therefore recommended. This effort should focus on existing silent or non-silent coverage as well as cyber coverage under non-cyber policies.

Finally, they warn about the pricing problem with regard to cyber risk: the current volume of the cyber premium - a market phenomenon - does indeed seem too low compared to the challenges posed by the cyber threat and the need to pool risk - the volume of the premium for France in 2018 is around €80 million (€2,700 million or €2.7 billion for the US).

For its part, the insurance industry has carried out a twofold analysis of the coverage to be offered to the sector organised by guarantee package and the quantification of this coverage? Insurers identified the guarantees that could be mobilized in the SME and ETI segments - the organization of guarantees being different according to the insurance companies by insurance package: Package 1 - crisis management: reconstitution of data losses, crisis management costs, systems reconfiguration costs, IT assistance, cause research; Package 2 - guarantees related to

operating losses and similar: EP, immaterial losses following the questioning of the approval, costs related to the loss of approval and the new application for approval, reimbursement of contractual penalties; Package 3 - guarantees related to the ransom: payment and or implementation costs. Package 4 - Guarantees related to deficiencies: supplier deficiencies following a cyber event at a third party and or customer deficiencies following a cyber event at a third party. The discussions did not focus on notification costs, administrative penalties and intangible assets.

The insurance, in its analyses, shows that for the liability part, the coverage is not only low in terms of amount but also raises the question of the relevance of a liability claim in terms of cyber claims. The problem of cross-conflicting actors - the fact that suppliers may be third parties between them - was excluded from the discussion. Nevertheless, some thought must be given to studying the chain of responsibilities, the possible remedies between suppliers in the event of non-compliance with a security obligation with regard to BoostAerospace's security standards. The insurance company is questioning the ability of policyholders to successfully recover in the event of a cyber security breach under civil liability. Insofar as security is only an obligation of means and no result, it remains uncertain that a security defect could lead to a supplier's liability being called into question, whether in terms of the state of the art, cyber maturity or standards not yet set, recognized and shared by the various players today. In addition, legal uncertainty arises at the national and international level. Finally, the assessment left to judges within the long delays of judicial time is not adapted to economic time. The recommendation is to clarify the framework for civil liability claims to better understand the financial legal risk of liability exposure due to a security breach in the aviation supply chain.

In terms of risk analysis, pricing and risk quality, insurers highlight their still limited understanding of cyber risk. At this stage, they do not have all the necessary and relevant information for their profession to analyse the quality of the insured's risk. Insurers recommend the development of their cyber risk assessment models and their ability to obtain more information from policyholders.

As part of this work, brokers considered the proposals that could be made, either as part of individual policies subscribed by all subcontracting companies or as part of a framework policy subscribed by principals for the benefit of the sector, while highlighting the capacity issue, particularly in the case of a framework policy. The individual and collective subject is not inseparable. A common foundation and a shared collective approach can be combined. The discussions also focused on the possible options of individual contracts, collective contracts or contracts on behalf of others, as well as the drafting of wording adapted and shared by insureds in the aeronautics industry.

Beyond the nature of the coverage, the brokers made proposals concerning the triggers at the heart of the coverage for the scenario - is one of the triggers - triggers of the coverage the cyber event with a notion of malicious intent understood in a sufficiently broad way not to be questioned and extended to the accidental option, the potential for questioning the aviation certification following a cyber event or the withdrawal of activity authorization by an administrative authority. The broker committee also proposes taking into account upstream and downstream supply chain actors to ensure the resilience of the whole. The objective is to guarantee the following losses: gross margin, temporary storage costs, expenses related to maintaining the activity, additional operating costs and crisis management.

The insurers' starting assumption in their scenario analysis was that 100% of subcontractors had purchased insurance. However, the current penetration of the cyber insurance market is very low for SMEs, SMIs, TWAs and SMEs. Cyber or traditional hedges represent only a part of the economic risk. It is therefore essential for principals to be able to insist on the implementation of shared and industry-applicable cyber security standards, adopted by the industry and recognised by various players, as well as compliance with cyber security clauses in subcontracts - insured, brokers, insurers and reinsurers. In contrast, the insurance market will be attentive to demonstrating the quality of the client's effective control.

We recommend the development of insurance coverage that will recognize the internal knowledge effort of the level of cyber risk exposure, investments in cyber security against recognized and shared standards, internal governance efforts implemented that demonstrate a level of cyber maturity and an ability to manage risk.

The principals should develop a communication towards the market to present these sectoral safety standards, that they be understood and recognized by the market to develop, for the benefit of subcontractors, insurance offers that are linked to safety standards and adapted to the needs of the sector.

XIII. Consolidated recommendations

Recommendations of the reinsurance committee

Recommendation 1: Define the cyber event so that insurance contract clauses are robust and recognized by all stakeholders in order to develop the clarity and robustness of contracts, particularly on the relevant clauses.

Recommendation 2. Continue the exercise of clarifying standard policies (damage, liability) to identify and reduce silent or non-positive exposures.

Recommendation 3. Improve tools and methods for calculating the accumulation and monitoring of exposures in relation to policy clarification and the pricing of cyber clauses in standard contracts.

Recommendation 4. Continue training, information, investment and awareness raising for all stakeholders regarding cyber risk and its systemic nature.

Recommendation 5. A process of reflection must be pursued in order to study and quantify financially the legal risk induced by the chain of responsibilities in terms of civil liability claims: the possible remedies between suppliers in the event of non-compliance with an obligation of security means.

Broker Committee Recommendations

Recommendation 6. The development of cyber risk profiling tools that assess the level of maturity of the insured in cyber security: taking into account the quality of the insured's cyber risk from a technical and governance point of view with the necessary financial elements

Recommendation of the insured

Recommendation 7. The development of sector-specific industrial cyber security standards recognized and shared by the insurance market.

Recommendation 8. The development of insurance coverage that will recognize the internal knowledge effort of the level of exposure to cyber risk, investments in cyber security with respect to recognized and shared standards, internal governance efforts implemented demonstrating a level of cyber maturity and an ability to manage risk