Entre le risque cyber et le risque de guerre, où se trouve la frontière ?

Avec le développement accru des nouvelles technologies dans tous les secteurs d'activités, les risques cyber ont pris une ampleur considérable. Par cyber risque, il faut entendre toute atteinte à des systèmes électroniques et/ou informatiques sous le contrôle d'une entreprise ou de ses prestataires, consécutive à un acte malveillant, une erreur humaine, des problèmes techniques ou un évènement naturel ou accidentel et entraînant des dommages pour l'entreprise[1] et/ou ses partenaires commerciaux. Les risques cyber existent par le seul recours aux technologies de l'information et de la communication utilisant des réseaux tel qu'Internet.

Les conséquences d'un incident cyber, volontaire ou accidentel, sont cruciales: coûts financiers importants, vol de données, cessation d'activités, coûts de réparation de systèmes endommagés, atteinte à la réputation et à l'image de l'entreprise victime.

Dans le secteur maritime, les problématiques que soulèvent les risques cyber sont plus larges. D'abord, parce qu'ils viennent en concours avec d'autres catégories de risques : les fortunes de mer et les risques de guerre. Ensuite, parce qu'un incident cyber sur un navire peut conduire non seulement à sa perte totale (explosion, incendie, échouement, abordage…) mais également à des catastrophes écologiques à la suite de ces événements.

Au regard de la menace que représente le risque cyber, tous les secteurs d'activités déploient d'importantes ressources et moyens pour y faire face. Chaque acteur économique dispose nécessairement d'une politique de gestion de risques et met tous les moyens en œuvre pour éviter des attaques cyber. Certains recourent à des assureurs pour se prémunir contre la part des risques que la prévention n'aurait pas suffi à éviter.

Mais quelles que soient les politiques de gestion de risques, les mesures de cybersécurité et les garanties d'assurances, quelques questions inexplorées demeurent: si le risque cyber peut coexister avec d'autres catégories de risques à l'instar des risques de guerre, un assureur qui offre une couverture pour cette dernière catégorie de risques peut-il être appelé à indemniser son client des conséquences d'une attaque cyber ? Ou inversement, un assureur cyber peut-il invoquer l'existence d'un risque de guerre dans le contexte d'une attaque cyber pour rejeter toute demande d'indemnisation de son client ? Ces questions qui illustrent les difficultés relatives à la frontière entre le risque cyber et les risques de guerre, font actuellement l'objet de l'affaire *Mondelez International, Inc. c/ Zurich American Insurance company* relative à

[1] Définition proposée par l'association des professionnels de la réassurance en France, in « Étude sur les cyber risques », juin 2016, p. 16.

l'indemnisation des conséquences de l'attaque cyber *NotPetya*, pendante devant une Cour suprême américaine.

Illustration du problème: *Mondelez International, Inc. c/ Zurich American Insurance company*

En 2017, l'attaque cyber *NotPetya* avait occasionné près de 3 milliards de dollars de pertes et de dommages[2]. La société *Mondelez International Inc*. était l'une des victimes de cette attaque. Le virus *NotPetya* avait infecté ses systèmes informatiques, entraînant le vol des données de plusieurs utilisateurs et paralysant 1700 secteurs et 24 000 ordinateurs lui appartenant. *Mondelez International* estime l'ensemble des pertes et dommages subies à plus de 100 millions de dollars.

Cette société était au moment de l'attaque, titulaire d'une police tous risques auprès de *Zurich American insurance Company*. La police tous risques couvrait tous dommages ou pertes physiques aux biens appartenant à l'assurée, en particulier les pertes physiques ou dommages aux bases de données électroniques, programmes ou logiciels, ainsi que ceux causés par l'introduction malveillante d'un code dans ses systèmes informatiques. Les garanties prenaient par ailleurs en compte les pertes supplémentaires résultant d'une éventuelle période d'interruption d'activités liée aux dysfonctionnements des installations informatiques. Cette police tous risques n'était pas nommément consacrée aux risques cyber mais comportait des clauses qui s'y rapportent. Sur la base de ce contrat, l'assurée a sollicité l'indemnisation des différents préjudices occasionnés par l'attaque cyber. Après avoir versé à son client une somme de 10 millions de dollars, l'assureur s'oppose finalement à la demande de ce dernier en invoquant une clause d'exclusion des risques de guerre contenue dans la police, soutenant que l'attaque cyber *NotPetya* aurait un lien avec un pouvoir politique et constituerait en conséquence un risque de guerre. Dans cette affaire, les juges doivent répondre à la question de savoir si une clause d'exclusion de risques de guerre, énoncée en des termes généraux dans une police d'assurance tous risques, peut être étendue à des attaques cyber prétendument diligentées par un État.

Au-delà de l'apparence relativement simple de ce problème, que l'on pourrait être tenté de réduire à une simple question de preuve, l'affaire soulève des difficultés dont l'issue pourrait considérablement influencer le marché de l'assurance cyber en cours de construction et aussi celui de l'assurance des risques de guerre et assimilés.

Cette affaire paraît en effet intéressante pour plusieurs raisons : d'abord, il s'agit du premier litige dans le domaine de l'assurance qui porte sur l'indemnisation de préjudices résultant d'une cyberattaque. Ensuite, c'est également la première fois qu'une compagnie d'assurance se prévaut de l'exclusion des risques de guerre pour contester la couverture d'une attaque cyber. L'issue de cette affaire pourrait avoir d'importants impacts sur le contenu et les limites des futurs contrats d'assurance cyber.

Du problème juridique posé aux juges, il ressort l'épineuse question de la distinction entre les risques cyber et les risques de guerre. Cette distinction est essentielle parce que d'elle, dépendront les limites des couvertures cyber et risques de guerre**.**

De la distinction entre les risques cyber et les risques de guerre

Les risques de guerre en matière d'assurance sont constitués dès lors que les intérêts assurés se trouvent dans une zone géographique perturbée ou menacée par un état de guerre réel et présent ou par des hostilités imminentes. Ils peuvent aussi être des faits concrets

[2] Artemis, « Merck & silent cyber impacts drove Petya industry loss: PCS », 7 nov. 2018.

caractéristiques de la guerre. Ainsi, dans un sens actif, les risques de guerre se présentent sous deux formes. La première forme désigne une situation conflictuelle réelle et actuelle caractéristique d'un état de guerre et la deuxième, des faits concrets qui se présentent comme des manifestations de la guerre. Ce sont des actes de guerre.

Le concept d'acte de guerre relève du droit international public. Il se caractérise par le recours par un État à la force, à toute action contre un autre État et qui apparaît clairement à ce dernier comme une déclaration de guerre, expressément ou implicitement[3].

Les cyber attaques n'impliquent pas un recours aux armes ni à la force. On pourrait tenter d'opérer une distinction en prenant en compte les mobiles ou l'origine de l'attaque pour définir deux catégories de cyber attaques, civiles et militaires en référence à la qualité des auteurs. Mais cette distinction peut se révéler arbitraire dans certaines circonstances dans la mesure où l'origine ainsi que le mobile des attaques sont souvent inconnus, notamment lorsqu'il n'y a pas de demande de rançon. Aussi est-il que, le paiement d'une rançon n'implique pas toujours un rétablissement sans conséquences des activités de l'entité victime. On peut en effet penser à l'hypothèse où les systèmes et équipements électroniques se retrouvent inexploitables à la suite de l'attaque et après même le paiement d'une rançon. N'est-on pas, dans cette situation, en présence d'une attaque détournée, si le but visé n'est pas qu'une simple demande de rançon ? Une doctrine majoritaire considère au regard de cette hypothèse qu'une cyberattaque peut, dans certaines circonstances, être qualifiée d'acte de guerre[4]. Mais concrètement, quand est-ce qu'une attaque cyber peut être considérée comme un acte de guerre et non comme un simple acte criminel ?

Quelques théories provenant du droit international public permettent de comprendre cette problématique. Le recours au droit international peut se justifier, en l'absence de législation nationale spécialement consacrée à la question et en raison du fait que le problème de la gestion du risque cyber dépasse la sphère géographique des États, tant que le risque lui-même n'est pas enfermé dans une zone géographique donnée.

Ainsi, tentant de répondre à la question posée, une partie de la doctrine estime que l'acte de guerre est constitué dès que l'attaque est raisonnablement susceptible de causer des blessures, mort d'hommes, dommages matériels ou destructions de biens[5]. Ici, le terme ''attaque'' est pris dans un sens premier et désigne tout acte de violence contre l'adversaire ou l'entité visée. Pour déterminer le caractère de guerre affectant l'attaque, cette doctrine propose de se référer, non pas à la nature spécifique de l'opération cyber, mais à ses conséquences[6]. Ainsi par exemple, une cyber attaque qui modifie le fonctionnement d'un système de contrôle et de recueil de données d'un réseau électrique et qui entraîne un incendie est constitutive d'acte de guerre. Dès lors que les conséquences ont un caractère destructif quelle qu'en soit l'ampleur, l'opération est qualifiée d'acte de guerre[7]. À ce propos, on peut citer le cas du virus informatique *Stuxnet* qui avait infecté les centrifugeuses iraniennes, causant de graves accidents et des pertes en vies humaines[8].

---

[3] Desiree Gargano, *an act of war: finding a meaning for what Congress has left undefined*, cité par Christopher M. Sanders, « The Battlefield of tomorrow, today: can a cyberattack ever rise to an "act of war?" », *Utah Law Review*, 2018, n°2, art.6, p. 511.

[4] Michael N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, Cambridge University Press, 2017, Règle 14, p. 84.

[5] Michael N. SCHMITT (ed.), Tallinn Manual 2.0 on the International Law applicable to cyber operations, préc., Règle 92, « definition of cyber attaque », p. 415.

[6] *Id*.

[7] *Ibid*.

[8] Justine Ferland « Cyber insurance – What coverage in case of an alleged act of war? Questions raised by the Mondelez v. Zurich case », *Computer law & security review*, vol. 35, 2019, p. 373.

Cette théorie précise que l'opération peut avoir porté sur des données appartenant à la victime ou dont celle-ci est responsable. Mais elle n'est pas moins constitutive de risque de guerre, dès qu'il en résulte des blessures ou morts d'hommes, des dommages à des biens ou leur destruction. La doctrine considère dans ce cas que ce sont en réalité les personnes victimes et les objets endommagés ou détruits qui constituent l'objet de l'attaque[9].

Cependant, quelle qualification convient-il de retenir lorsqu'au contraire, une cyber attaque détruit des données et provoque ainsi le dysfonctionnement des systèmes informatiques, sans détruire les équipements eux-mêmes ? Une doctrine majoritaire considère dans ce cas, à juste titre, que les critères de qualification qui font état d'au moins un dommage, n'étant pas réunis, l'attaque ne saurait être qualifié d'acte de guerre[10].

Une doctrine intermédiaire propose d'opérer une distinction en vérifiant s'il y a ou non une nécessité de remplacer le système informatique affecté ou l'un de ses composants à la suite de l'événement cyber. Ainsi, si une réparation sous la forme d'un remplacement de système ou du composant essentiel au fonctionnement du système est nécessaire pour restaurer sa fonctionnalité, alors un dommage a pu être causé et par conséquent l'événement cyber qui en est la cause est une cyber attaque constitutive d'acte de guerre[11]. On en déduit que si aucun remplacement n'est nécessaire pour restaurer le système, il n'y a donc pas de destruction et on serait alors dans le cas d'une cyber attaque pure.

La frontière entre le risque cyber et le risque de guerre apparaît alors très ténue. Une police risque de guerre pourrait facilement être mise en cause dans le contexte d'un événement cyber, au regard des solutions qui viennent d'être exposées, alors même qu'elle ne vise pas ce type d'événement.

Incidence sur les couvertures risques de guerre et risques ordinaires

La possibilité que des risques cyber soient qualifiés dans certaines circonstances de risques de guerre, peut avoir une incidence sur les couvertures risques de guerre. Le problème ne se pose pas véritablement pour les couvertures risques ordinaires[12]. Car celles-ci comportent toujours une clause d'exclusion tant des risques cyber[13] que des risques de guerre[14], de telle sorte la qualification des risques cyber en risques de guerre et inversement s'inscrit dans l'une ou l'autre des exclusions.

Le problème est sans doute plus important en matière de l'assurance des risques de guerre. Il est vrai qu'en pratique, les conventions spéciales corps et facultés (la garantie *Waterborne* et la garantie Étendue) contre les risques de guerre excluent les risques cyber des garanties offertes. Cependant, dans la mesure où le risque de guerre peut prendre la forme d'un risque cyber, l'application de la clause d'exclusion cyber LC 380 serait-elle suffisante pour contester des réclamations fondées sur un événement cyber caractéristique d'un risque de guerre ? Il serait nécessaire de réviser cette clause.

La qualification du risque cyber a aussi une incidence sur l'assurance du risque de piraterie. En effet, les polices risques ordinaires et risques de guerre peuvent être affectées en ce qui concerne les garanties offertes contre le risque de piraterie. Le marché français opère pour leur couverture, une distinction entre la piraterie dite lucrative et la piraterie à caractère politique ou

---

[9] Michael N. SCHMITT (ed.), *Tallinn Manual 2.0 on the International Law applicable to cyber operations*, préc., Règle 92, préci., (6), p. 416.

[10] Djemila Carron, *L'acte déclencheur d'un conflit armé international*, Thèse, Université de Genève, 2015, p. 237.

[11] William H. Boothby, « Where do cyber hostilities fit in the International Law maze?», *in* Hitoshi Nasu, Robert McLaughlin (ed.), *New technologies and the Law of armed conf*lict, Asser Press, The Hague, 2014, p. 59-73, (61-62).

[12] Sauf dans le cas de la couverture du risque de piraterie.

[13] Par application de la Clause CL 380 du 10 nov. 2003.

[14] Police d'assurance maritime sur corps de tous navires, tous risques du 1er janv. 2012, art. 1.2.3. ; police française d'assurance maritime sur facultés, tous risques du 1er juil. 2009, art. 7,7°.

se rapportant à la guerre. La piraterie lucrative est couverte par la police risques ordinaires et la piraterie à caractère politique ou se rapportant à la guerre est prise en charge par la police contre les risques de guerre[15].

Aujourd'hui, les méthodes d'attaque des pirates ont évolué grâce aux nouvelles technologies. Les pirates ont la possibilité d'agir à distance pour prendre le contrôle des navires en utilisant l'internet. La piraterie peut ainsi reposer sur une attaque cyber. Des actes relevés dans le golfe de Guinée ont déjà montré que des outils de *reporting* mis en place pour protéger la navigation pouvaient être détournés à leur avantage par des pirates[16]. Ces derniers ont en effet la possibilité de détourner des données informatiques relatives à la position et aux itinéraires des navires, d'identifier le contenu des cargaisons pour cibler les navires à attaquer[17].

Or conformément aux critères de qualification proposées par la doctrine, un événement cyber peut avoir les caractères d'un acte ou fait de guerre dès que les équipements électroniques de communication et de navigation subissent un quelconque dommage du fait de l'attaque cyber. Cette qualification opère indépendamment de l'origine de l'attaque.

Ainsi la piraterie lucrative réalisée à travers une attaque cyber et causant un dommage, quel qu'il soit, serait qualifié de risque de guerre au même titre que la piraterie politique déjà assimilé au risque de guerre.

Dans ce contexte, la distinction entre la piraterie lucrative et la piraterie à caractère politique n'aurait plus de portée pratique réelle. La maintenir, reviendrait pour l'assureur des risques ordinaires à exclure non seulement les risques cyber mais aussi la piraterie lucrative à caractère cybernétique, dommageable ou non. Ce qui aboutirait implicitement à une exclusion de la piraterie lucrative si l'on admet que la piraterie traditionnelle fait progressivement place à la piraterie basée sur les outils informatiques et donc à caractère cybernétique.

Par ailleurs, un exercice de délimitation des contours des garanties s'impose. Car la piraterie peut être qualifiée de risque cybernétique si elle s'appuie sur des cybermalveillances, de risque de guerre en plus d'être cyber, en présence d'un dommage aux équipements ou en cas de blessures et/ou atteinte à la vie.

ADAM ASSURANCES - 33, Allées de Chartres – 33000 Bordeaux

www.adam-assu-mar.com
Le Lab – Recherches et innovations en assurances maritimes et transports
En partenariat avec
le Centre de droit maritime et océanique, Nantes
et le Centre de recherche et de documentation européennes et internationales, Bordeaux

Patrice A. EDORH-KOMAHE
pedorh-komahe@adam-assu-mar.com

Publié le 22 octobre 2019

[15] L'antenne, Assurance : la couverture "Piraterie" toujours en débat, https://www.lantenne.com.
[16] ISEMAR, « Piraterie maritime : la maîtrise du risque ? », Note de Synthèse N° 199 - Avril 2018.
[17] *Id*.