L'AUTONOMIE STRATÉGIQUE FACE AU CYBER-RATING

Une nouvelle dépendance émerge…

La crise mondiale que nous traversons fait constater au grand public deux éléments structurants de notre organisation économique. Le premier est le rôle du numérique en tant qu'amortisseur économique ; le second est la conséquence d'une multi-dépendance des entreprises et des États induite par leurs chaines d'approvisionnement dans un monde globalisé. En effet, n'alarmant que les spécialistes, le changement de pavillon d'Alstom ou de Latécoère impose des pertes plus larges que les éventuelles pertes d'emplois. Celles-ci apportent toutefois beaucoup moins d'audiences qu'une rupture d'approvisionnement en masques ou en gel hydro-alcoolique, préoccupation beaucoup plus concrète pour les citoyens. **L'autonomie stratégique** a ainsi glissé des comités de la défense française et européenne vers les éléments de langage politique diffusés plus largement. Cette autonomie est souvent confrontée à de nouvelles menaces très discrètes et patiemment construites à travers les années par nos « partenaires » commerciaux internationaux et contre les libertés de notre tissu économique.

Parmi les sources de menaces, nous trouvons les incontournables et controversées agences de notations financières. Plus que centenaires et malgré l'échec de la crise de 2008, elles se renouvellent dans la notation extra-financière[1] qui intègre discrètement une nouvelle composante : **« la notation cyber ».**

Les études en référence et les réflexions à suivre aideront à éclairer le lecteur sur ce qu'est l'autonomie stratégique et rappelleront comment les agences de notation financière sont devenues incontournables et toutes puissantes. Nous appliquerons ensuite une extrapolation aux agences de cyber-rating, et l'introduction à moyen terme d'un nouveau rapport de force sur nos chaines d'approvisionnement.

De l'autonomie stratégique

Suite à la guerre froide et dans un monde où les états, les économies, la recherche, et les lois deviennent de plus en plus « multi et inter dépendant », il n'est plus réellement envisageable de retrouver une véritable indépendance[2]. La France fait alors surgir le concept d'**autonomie stratégique**, avec un sens autoporté et un manque de définition juridique[3]

[1] Social, environnement, gouvernance.

[2] « Elle supposait la capacité d'agir seul partout, de se défendre seul, de pouvoir faire porter seul sa voix partout dans le monde. Dans un monde incertain, ouvert et flexible, le monolithisme paie beaucoup moins. » ; Rapport de l'Institut Montaigne sur « La sécurité extérieure de la France face aux nouveaux risques stratégiques » www. institutmontaigne.org/publications

[3] Le *GRIP* est le « G*roupe de recherche et d'information sur la paix et la sécurité ». https*

claire bien qu'il soit maintenant le premier objectif du programme européen de développement industriel dans le domaine de la défense (EDIDP).

---

*« Pour pouvoir faire face aux menaces de demain et protéger ses citoyens, l'Europe doit accroitre son **autonomie stratégique**[4] »*
(Commission européenne – 2017).

L'autonomie stratégique est présente dans les livres blancs sur la défense nationale depuis 1994[5-6] où elle combine : la « liberté d'appréciation », la « liberté de décision » et la « liberté d'action du chef de l'état ». Les travaux européens[7] y ajouteront la « sécurité des approvisionnements » en 2016.
Le rapport du GRIP[8] de janvier 2018 identifie trois composantes à l'autonomie stratégique :

- politique : « la capacité de prendre des décisions dans le domaine de la défense et de les exécuter sans en être empêché par d'autres puissances » ;
- opérationnelle : « la capacité de mener, de façon autonome, des opérations militaires, en rapport avec l'objectif poursuivi, dans la durée » ;
- industrielle : « la capacité de produire les équipements militaires nécessaires à l'accomplissement des opérations militaires précitées » ;
  Ce concept est donc introduit dans le débat par la « Défense », et dans un contexte de « guerre économique » multiforme à peine dévoilée. Depuis 2017, il s'est étendu à la sphère civile (économique, industrielle, et juridique…). L'autonomie stratégique prend ainsi naissance en tant que réponse à un besoin d'évolution du concept devenu inapplicable d'indépendance pleine et entière. Elle remplace ainsi le précepte du « seul dans l'analyse, seul dans la prise de décision, seul dans l'action, et avec ses propres moyens d'action ». Elle est une composante d'une transformation déjà entamée des règles du jeu géopolitique.

Fais tes affaires toi-même, tu ne seras pas trahi.
Proverbe nigérian ; Les Haoussas en proverbes (1905)

Le rapport du GRIP nous aide à combler ce manque : Autonomie Stratégique : Autonomie *stratégique : le nouveau Graal de la défense européenne*, Frédéric Mauro, 01/2018.

[4] Communication de la Commission européenne du 7 juin 2017 sur le lancement du Fonds européen de défense, COM (2017) 295 final, p. 2, ec.europa.eu/transparency/regdoc/rep/1/2017/FR/COM-2017-295-F1-FR-MAIN-PART-1.PDF

[5] Page 52 : « Notre autonomie stratégique sera dans ce cadre de plus en plus tributaire de notre aptitude à maîtriser quelques fonctions clés, hors nucléaire proprement dit : - l'intelligence des situations, notamment par le renseignement qui permet la prévision et l'appréciation autonome des événements et donne ainsi la capacité de décider rapidement, en opérant des choix éclairés ; - la maîtrise des situations complexes, où se mêlent les dimensions politiques, militaires et régionales du point de vue de la stratégie, les dimensions multinationales et interarmées dans le domaine militaire ; la mobilité stratégique, pour être libre de nos mouvements, et pouvoir projeter les forces en temps utile au bon endroit. »

[6] « Le Livre blanc sur la défense et la sécurité nationale de juin 2008 assimile, dans le prolongement de son prédécesseur de 1994, l'autonomie stratégique à la somme de trois libertés : « la liberté d'appréciation », « la liberté de décision » et la « liberté d'action du chef de l'État »15 sans toutefois définir de façon plus précise ce que recouvrent ces composantes.

[7] « The future of EU Defence research », Parlement européen, 30 mars 2016, p. 27.

[8] Rapport du GRIP : *Autonomie Stratégique : Autonomie stratégique : le nouveau Graal de la défense eurpéenne*, Frédéric Mauro, 01/2018.

Rechercher l'autonomie stratégique dans les domaines vitaux et essentiels (d'un état, d'une entreprise ou d'une ONG …) revient donc à :

- rompre les dépendances avec tous les acteurs s'interposant à l'une des trois libertés (anticipation, décision, action) ;
- construire de nouvelles interactions de confiance en s'appuyant à minima sur deux nouveaux critères forts, **« la communauté de destin »** et la **« communauté de dessein »,** indispensables à la sécurité des chaînes d'approvisionnements.

« La communauté de destin est celle qui est provoquée par les réalités extérieures aux individus et qui s'impose à eux avec force ; au premier rang de celles-ci, on trouve la réalité territoriale dès lors qu'on n'a pas les moyens de la quitter. De son côté, la communauté de dessein est celle que l'on choisit en fonction de ses intérêts ou de ses convictions. Pour apparaître, elle suppose que les personnes qui ont des intérêts communs aient les moyens de se repérer et de se rencontrer. »

Agence de notation : le "First mover takes all"

L'objectif n'est pas de démontrer les bénéfices ou les problèmes induits par les agences de notation financières dont la mission est d'évaluer le risque de défaut d'un emprunteur sur ses dettes financières. Ceci est parfaitement illustré dans de nombreuses études réalisées à la suite de la prise de conscience qui a eu lieu lors de la crise financière de 2008. Parmi ces études, on notera principalement celles du Sénat de juin 2012[9] et l'analyse produite par l'École de Guerre Économique de juin 2019 sur l'information extra-financière[10]. Sans revenir sur les derniers scandales des années 2000, nous verrons les points « historiques » les plus saillants qui ont amené à ce quasi-monopole mondial des entreprises américaines sur les capacités de financement des états et des entreprises à travers le monde. Ceci posera le contexte pour mieux anticiper ce que pourrait être une dérive des agences de cyber-rating.
Les premières sociétés d'analyse de crédit (pas encore de système de notation) datent de 1837 et étaient une des réponses aux dysfonctionnements du système financier. Le marché s'est progressivement structuré pendant presque un siècle jusqu'à l'apparition des premiers ouvrages posant les bases théoriques des futures agences de notation (John Moody ; Analysis of Railroads Investments ; 1909). Ces dernières apparurent aux alentours des années 1920 avec les premières notes des sociétés Poor's Publishing Company (1916), Standard Statistic Company (1922) et Fitch Publishing Company (1924). L'intérêt porté par les investisseurs pour ces sociétés pousse les États-Unis à l'encadrer par des textes précis. Une première consolidation de ce marché est alors en marche pendant les années 30.
La Seconde Guerre mondiale a été l'opportunité (cynique ?) d'accroitre la vélocité de ce marché vers l'Europe grâce entre autres, aux positions acquises par les États-Unis avec les accords de Bretton Woods et le plan Marshall tout aussi utile pour les USA que pour l'Europe

[9] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur)
[10] *Information extrafinancière* : Une sphère d'influence, une nouvelle arme de guerre économique, un nouveau terrain de conquête hégémonique, Ecole de Guerre Economique, Juin 2019.

en pleine reconstruction. Aidés par ce terreau favorable et peu d'initiative concurrentielle crédible, les trois noms emblématiques maintenant connus comme Standard and Poor's, Moody's et Fitch ont maintenu leur position oligopolistique jusqu'à détenir et conserver 94% du marché mondial.
Ce n'est qu'en 1975 et après avoir eu le temps d'établir un standard de fait qu'apparaît aux USA, la certification de NRSRO (Nationally Recognized Statistical Rating Organization) qui autorise une société à attribuer une note. Avec un modèle économique laissant la place aux doutes (les notations sont payées[11] par les organismes qui souhaitent se financer sur les marchés de capitaux et non les investisseurs. Elles sont utilisées par les investisseurs pour éclairer et orienter leurs choix. On parle pour les agences de notation d'un modèle « émetteur-payeur »), ce n'est qu'en 2003 que les USA commencent à élargir (si peu) la liste NRSRO à plus de concurrence. L'Europe répondra en 2005 avec la création de l'autorité européenne des agences de notation qui distribuera plus largement le précieux sésame[12].
La surreprésentation américaine dans ce marché a pourtant été troublée par le rachat de Fitch en 1997 par FIMALAC, un groupe français qui a démarré une activité de notation en 1992. Cependant il semble compliqué d'imposer une vision des choses à la française dans ce marché anglo-saxon par essence, ce qui a fait dire à son président : *« Il ne faut pas se bercer d'illusions : nous vivons et continuerons encore longtemps à vivre dans un monde anglo-saxon![13] »*. L'aventure de FIMALAC dans la notation prend fin en 2018 avec la vente d'un dernier lot de parts sociales à un groupe américain, cédant ainsi la dernière position forte française sur cet échiquier économiques.
À ce jour, neuf agences seulement ont le NRSRO qui permet d'intervenir aux USA là où trente-cinq se partagent le marché européen. Les 3 agences historiques américaines ont maintenu leur stratégie d'oligopole, et règnent toujours en maître[14] sans retour en arrière possible à court terme[15] de l'avis même du Sénat français.

« Suite à la crise financière, la SEC a élargi le champ des agences agréées à neuf agences, mais n'a pas attribué son label aux petites agences européennes, ce qui contrarie leurs activités sur le territoire américain. Seules de petites agences américaines ont été labellisées par la SEC. Si l'obligation de notation était mise en œuvre, les entreprises européennes devraient donc recourir à l'une des petites agences américaines afin d'avoir accès aux investisseurs anglo-saxons. »
Marc Ladreit de Lacharrière, 2012, président de FIMALAC, premier actionnaire et président de FITCH

Pourtant les prix montent sans pour autant être suivis d'une hausse de la qualité. *« L'analyste note beaucoup trop d'organismes pour que cela soit sérieux,* il n'a pas de temps d'approfondir *»*. Standard and Poor's et Moody's détiendraient ensemble 80 % des parts de

[11] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur).
[12] USA = 9 agences ; EU > 30 agences.
[13] ibid
[14] Les failles des agences de notation, Ilanah JOSPÉ, Juliette MONTEFIORE, Émeline TRIN.
[15] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur).

marché mondial et Fitch 15 %[16]. Autrement dit, les six autres acteurs américains et trente-deux autres européens se partagent les 5% du marché restant avec les agences asiatiques également présentes.

3 agences pour 95% du marché mondial.
32 agences pour le marché européen.

Au lendemain de la crise financière de 2008, le monde s'est aperçu de la fébrilité du système de notation. Des entreprises bien notées n'ont pas survécu à cet évènement. Cependant encore aujourd'hui, ce système fait toujours référence, car il répond à un besoin de lisibilité de la complexité. Nous sous-traitons donc à des organismes privés battant pavillon américain (à plus de 94% du marché), le rôle de régulateur, sans pouvoir nous en défaire. Voici une faiblesse manifeste dans notre indépendance stratégique. En effet, *« la zone euro emprunte des sommes gigantesques aux États-Unis. Cela ne signifie pas que ce sont les Américains qui prêtent, mais des gestionnaires de fonds qui gèrent des sommes qui viennent du Golfe persique »*[17].
Le taux d'emprunt dépend directement de cette note.
Le rapport du sénat[18] de 18 juin 2012 décrit le rôle de tiers de confiance de ces agences, réduisant les marges d'incertitude dans les risques financiers pris par les assurances et les banques pour leurs clients (entreprises ou états). Ce rôle est *« une quasi-mission de service public »*[19] sans le moindre contrôle des autorités étatiques. Et les tentatives de manœuvres pour se désenclaver peinent à convaincre.

« La notation est un point de passage imposé par les pouvoirs publics et les investisseurs sans alternative crédible à court terme… De manière rétrospectivement contestable, les pouvoirs publics ont fait des agences de notation de quasi-régulateurs… On a délégué de manière diffuse une mission de service public de Standard and Poor's, Moody's et Fitch, sans cahier des charges, sans contrôle et sans exigence de résultat… Les agences de notation sont devenues incontournables, sans retour en arrière possible à court terme. »[20]

[16] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur)
[17] http://www.senat.fr/rap/r11-598-1/r11-598-11.pdf , Audition devant la mission commune d'information du Sénat le 9 mai 2012. « le marché de la notation va être très important dans les années à venir, les endettements des États, des collectivités locales et des entreprises ne faisant qu'augmenter. L'Europe – et notamment la zone euro – se trouve dans une situation d'une très grande difficulté puisque, structurellement, les politiques menées par chacun des gouvernants de chacun de ces pays, en dehors de quelques exceptions, depuis vingt ans, ont conduit ces pays à financer leur croissance en s'endettant d'une manière importante. La zone euro emprunte des sommes gigantesques. Où les emprunte-t-elle ? Elle les emprunte pour le moment aux États-Unis. Cela ne signifie pas que ce sont les Américains qui prêtent mais ce sont les gestionnaires de fonds, aux États-Unis, qui ont en dépôt des sommes qui viennent du Golfe persique et qui les gèrent », Marc Ladreit de Lacharrière, 2012, président de FIMALAC, premier actionnaire et président de Fitch
[18] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur)
[19] Ibid.
[20] Ibid.

Parmi les problèmes mis en évidence par ce rapport il y a :

- **La transparence** : encore aujourd'hui, les méthodologies d'analyses sont propres à chaque agence et les documents publiés sont jugés trop complexes ;
- **La délocalisation du droit** : Les agences imposent aux émetteurs de recourir à des contrats de droits anglo-saxons ;
- **La pertinence des analyses produites** par des analystes peu expérimentés[21] ;

Standard & Poor's en Europe	< 2 ans	2 à 5 ans	> 5 ans
Entreprises et institutions financières	13 %	35 %	51 %
Autres	10 %	14 %	76 %
Souverains et assimilés	11 %	38 %	52 %
Produits structurés	11 %	53 %	36 %
Total	**12 %**	**39 %**	**49 %**
Moody's en Europe	**< 2 ans**	**2 à 5 ans**	**> 5 ans**
Entreprises	16 %	48 %	35 %
Institutions financières	22 %	44 %	34 %
Souverains et assimilés	30 %	48 %	22 %
Produits structurés	13 %	52 %	36 %
Total	**17 %**	**49 %**	**49 %**
Fitch en Europe	**< 2 ans**	**2 à 5 ans**	**> 5 ans**
Entreprises	17 %	54 %	29 %
Institutions financières	17 %	54 %	29 %
Produits structurés	7 %	74 %	19 %
Total	**13 %**	**59 %**	**28 %**

Figure 1: ancienneté des analystes de S&P, Moody's et Fitch en Europe (2009-2010)[22]

- **La distorsion de notation** : *« EADS a dû faire appel à un conseil en notation pour rétablir sa note, injustement fixée à BBB+ alors que Boeing bénéficiait d'un A+. La marge comptable présentée par Boeing était basée sur des comptes aux normes américaines (US GAAP). Celle d'EADS l'était sur des comptes aux normes internationales (IFRS). Après retraitement, EADS a pu faire valoir que l'entreprise méritait un A, et non un BBB+. »*[23]
- **Le modèle économique émetteur payeur** qui induit un doute sur le conflit d'intérêts.

  Il n'est donc pas inconcevable que ces problèmes connus et acceptés par tous puissent être exploités en toute impunité dans le cadre d'une action d'influence à l'encontre des actifs économiques d'un organisme.

[21] Ibid 62 % des analystes affectés à la notation des entreprises avaient moins de cinq années d'ancienneté en 2009-2010 et, seulement 14 % des analystes de Fitch au niveau mondial disposaient de la certification externe de « Chartered Financial Analyst ».
[22] Ibid.
[23] Ibid.

« La dictature des notes »[24]

Malgré cette liste de problèmes, deux dogmes semblent irrévocables : les systèmes de notation comme unique mode de régulation d'une part, l'acceptation des « tiers de confiance privés » comme régulateurs implicites de la vie économique d'autre part. Cet engouement ne se limite plus désormais au domaine financier. Toutes les activités ayant un rôle dans le circuit économique peuvent être notées. Le rapport de l'École de Guerre Économique de juin 2019 « Information extra-financière : Une Sphère d'influence : une nouvelle arme de guerre économique, un nouveau terrain de conquête hégémonique » traite de trois domaines extra-financiers (Environnement, Social et Gouvernance), mais précise que tout domaine sans norme associée peut être couvert.

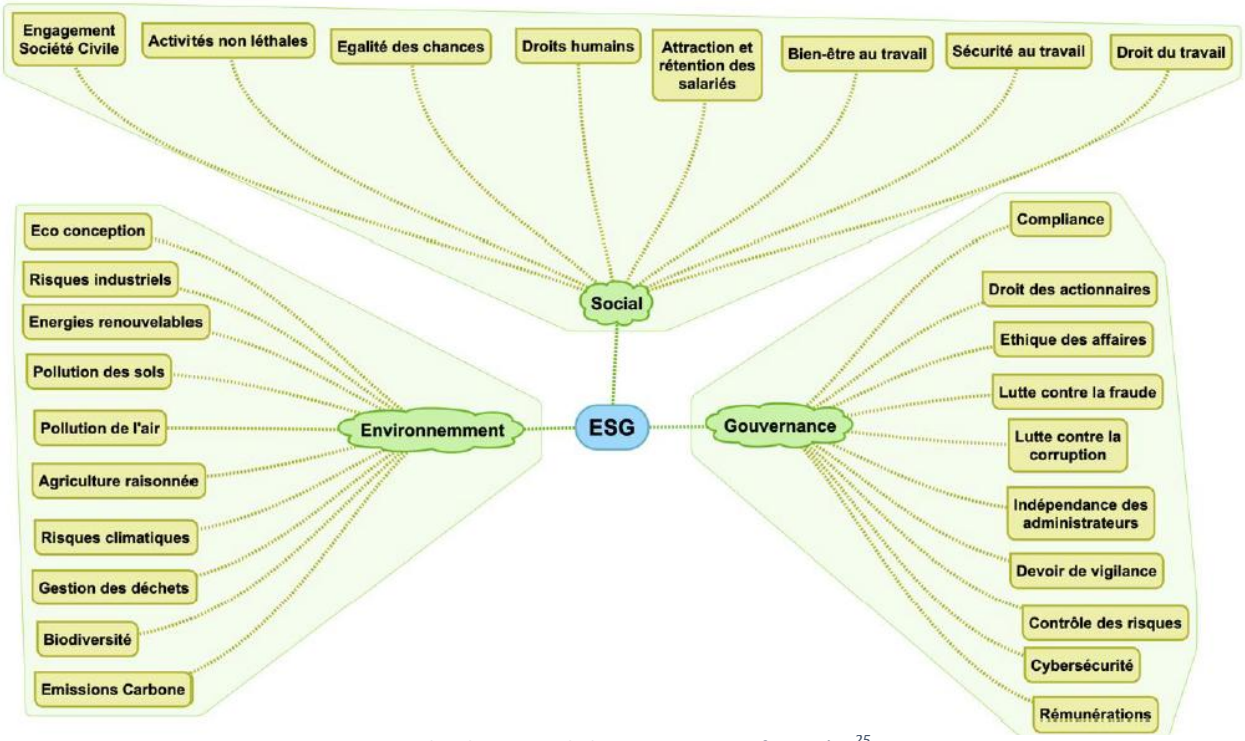

Figure 2: les domaines de la notation extra-financière[25]

Cette absence de norme est aisément remplacée par des standards de fait, promus par les acteurs économiques pouvant tirer un avantage à être la référence de leur marché. La note n'intéresse plus uniquement les Directeurs Administratifs et Financiers, mais également les bailleurs et les clients qui souhaitent garder leur conscience tranquille.
Aux yeux du grand public, la réputation d'une entreprise est souvent plus liée à un véhicule émotionnel que rationnel. Une mauvaise note peut autant nuire à l'entreprise ciblée qu'être utile à son concurrent. La note rassure ou inquiète, et tant pis pour la méthodologie employée qui aboutit au résultat.

[24] Gerard AMPEAN, auteur de la « comédie de la notation », *Interview « Standard&Poor's, Moody's, Fitch* : des agences de notation en roue libre ? » du 7 février 2019.
[25] Domaine de la notation extra-financière, source EGE, juin 2019, « Information extrafinancière : Une Sphère d'influence : une nouvelle arme de guerre économique, un nouveau terrain de conquête hégémonique » met en évidence les ESG pour Environnement, Social et Gouvernance.

…susciter des courants émotionnels et psychologiques qui travailleront pour eux [les commerciaux]. Au lieu de s'attaquer de front aux résistances des acheteurs, ils cherchent à les supprimer. À cet effet, ils créent les circonstances qui, en canalisant les courants émotionnels, vont produire la demande.
Edward BERNAY, Propaganda

« Les enjeux extra-financiers étant par nature universels, il ne faut donc pas s'étonner que tout le monde cherche à se les approprier et à les imposer aux autres…on observe depuis 20 ans dans le domaine de la notation extra-financière des mouvements de troupes dans ce qui était il y a encore peu une industrie extrêmement fragmentée»[26]. Là encore des consolidations anglo-saxonnes prennent le dessus.
Le marché du cyber-rating a vu le jour en 2013 et porte lui aussi dans son ADN des dérives qu'il ajoute à celles de ses ainés.

La notation du risque cyber

L'explosion de la consommation des services numériques apporte une diversification des menaces cyber et une expansion de la surface d'attaque souvent mal comprise par les décideurs. La prise de conscience de l'existence réelle des attaques cyber tend à se réaliser et à gagner suffisamment en importance pour faire partie des préoccupations mondiales majeures. Aujourd'hui, les risques numériques figurent parmi les dix risques les plus préoccupants au niveau international[27] comme le note le rapport sur les risques globaux du Forum Économique Mondial (2020).

Figure 3: The Global RisksReport 2020, World Economic Forum

[26] ibid.
[27] The Global RisksReport 2020, World Economic Forum, Insight Report 15th Edition, In partnership with Marsh & McLennan and Zurich Insurance Group.

TOP 10 RISKS IN FRANCE

Source: Allianz Global Corporate & Specialty.

Figures represent how often a risk was selected as a percentage of all responses for that country.

Respondents: 77

Figures don't add up to 100% as up to three risks could be selected.

Rank		Percent	2019 rank	Trend
1	**Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)**	**49%**	1 (41%)	=
2	Business interruption (incl. supply chain disruption)	**48%**	2 (40%)	=
3	Fire, explosion	**35%**	3 (29%)	=
4	Natural catastrophes (e.g. storm, flood, earthquake)	**30%**	4 (28%)	=
5	Product recall, quality management, serial defects	**18%**	8 (12%)	▲
6	Changes in legislation and regulation (e.g. trade wars and tariffs, economic sanctions, protectionism, Brexit, Euro-zone disintegration)	**17%**	5 (26%)	▼
7	Political risks and violence (e.g. geopolitical conflict, war, terrorism, civil commotion)	**13%**	NEW	▲
7	Theft, fraud, corruption	**13%**	10 (10%)	▲
9	Loss of reputation or brand value	**10%**	8 (12%)	▼
9	Market developments (e.g. volatility, intensified competition/new entrants, M&A, market stagnation, market fluctuation)	**10%**	6 (18%)	▼

Figure 4: Baromètre des risques 2020 d'Allianz

Les entreprises souhaitent donc couvrir ce nouveau risque en le transférant aux assurances. Ces dernières se retrouvent confrontées à des risques souvent difficiles à évaluer pour les statisticiens qui manquent de données[28]. *« Les risques cyber font encore plus peur aux assureurs qu'aux assurés ! … Il existe ainsi clairement une nécessité de voir émerger un standard commun pour faciliter le dialogue entre assureurs, courtiers et acheteurs[29]».* Les agences de notation cyber apportent une réponse à ce nouveau besoin faisant un marché mondial estimé à ce jour à plus de 500 millions d'euros mais pouvant influencer bien plus.

« Une agence de notation cyber est un tiers neutre qui donne une notation basée sur des critères objectifs concernant le niveau de cyber-sécurité de la cible. Cela donne une perception de la réalité basée sur des critères mesurables de l'extérieur sans l'intervention active de la cible… C'est un élément de la confiance parmi d'autres…[30] » - François-Xavier Vincent, OODRIVE

À l'instar de leurs homologues de la finance, les premières agences de notation cyber viennent des États-Unis et reprennent les mêmes méthodes pour évaluer l'exposition des

[28] Agences de notation, pour une profession règlementée (Juin 2012). Synthèse du rapport sur les agences de notation. Frédérique ESPAGNAC (présidente) et Aymeri de MONTESQUIOU (rapporteur) ; Les agences de notation financières sont maintenant un point de passage obligé. Même les banques centrales font appel aux agences « pour s'assurer de la solidité des actifs des banques et des sociétés d'assurance ainsi que de la réalité des risques pris ».

[29] COMMENT « DÉBLOQUER » LE MARCHÉ DE L'ASSURANCE CYBER EN FRANCE ? Par Charles d'AUMALE (1997), François GRATIOLET (1999), Stéphane SOLLAT (2009), François-Xavier VINCENT, juin 2017.

[30] *Interview* de François-Xavier Vincent, CISO & DPO de Oodrive.

entreprises aux risques cybers. Comme l'indique clairement Moody's et S&P qui intègrent maintenant le cyber dans leur notation : **l'objectif est de créer un standard de fait**[31].

Moody's Corporation (NYSE:MCO) and Team8, a leading cybersecurity think tank and company creation platform, announced today that they have formed a joint venture to establish a global standard for evaluating and assessing cyber risk for enterprises.
Press Release, Moody's, Le 27 juin 2019

Le rapport d'information du député Éric BOTHOREL du 14 novembre 2019[32] indique qu'il est tout aussi compliqué d'estimer les coûts des dommages causés par une cyber-attaque que de définir un indicateur qui permettrait de mesurer le niveau de cybersécurité. Il y a une réalité technique et organisationnelle à ce constat. Cependant, c'est oublier un peu vite que s'il y a un couple « besoin + budget », il y aura toujours une solution innovante pouvant être achetée, même si celle-ci n'est pas conforme à une vision académique de ce que devrait être la performance[33]. Les agences de notation cyber profitent de cette opportunité. Elles pourraient d'ailleurs s'appuyer sur un ensemble de références documentaires comme, le framework du NIST, les règles d'hygiène de l'ANSSI, l'Information security indicators de l'ETSI, afin de s'approcher d'une **mesure de la performance sécurité réalisable à un coût acceptable** pour les clients. Ce dernier point doit également faire partie de l'équation. Pour des raisons de coût, aucune organisation n'accepterait d'investir dans un état des lieux exhaustif de l'intégralité de son SI.

La note se base sur ce qui mesurables de l'extérieur. Le système de management de la sécurité du système d'information de l'organisme noté est ainsi occulté, au mieux il peut être partiellement imaginé. En contrepartie le CISO (Chief Information Security Officier) y trouvera un indicateur simple à remonter à son COMEX qui pourra l'utiliser comme :

- un **indicateur concurrentiel** : un moyen de comparaison en continu par rapport aux autres acteurs d'un même secteur d'activité.
- un **argument de vente** : un élément de communication et de confiance à produire à ses clients et investisseurs.
- un **moyen de ségrégation et de sélection** : une évaluation des fournisseurs et/ou l'accès à des marchés règlementés (appels d'offres publics). Il s'agit là de la principale demande des clients d'acteurs comme Security Scorecard[34].

---

[31] Moody's Corporation (NYSE:MCO) and Team8, *a leading cybersecurity think tank and company creation platform, announced today that they have formed a joint venture to establish a global standard for evaluating and assessing cyber risk for enterprises. Chris Heusler, Chief Commercial Officer at S&P Global Ratings, said "…* Their approach to cyber risk complements ourRatings360 product offerings*, and can also be leveraged across S&P Global."*

[32] RAPPORT D'INFORMATION DÉPOSÉ PAR LA COMMISSION DES AFFAIRES EUROPÉENNES (1) sur l'avenir de la cybersécurité européenne ET PRÉSENTÉ PAR M. ÉRIC BOTHOREL, Député, Enregistré à la Présidence de l'Assemblée nationale le 14 novembre 2019.

[33] Ibid - la définition d'un indicateur qui permettrait de mesurer le niveau de cybersécurité continue de poser problème. Les indicateurs existent, mais c'est peut-être leur foisonnement et l'absence de consensus sur les paramètres à intégrer qui empêchent l'émergence d'une seule mesure suffisamment consensuelle pour assurer son utilisation large.

[34] François Samarcq, directeur des ventes de SecurityScorecard, qui précise qu'il s'agit là de la principale demande des clients de la société, devant l'auto-évaluation et, chose de plus en plus fréquente dans le cas de fusions-acquisitions. Source : *CyberRisques n°1* – 1er trimestre 2020 .

- un moyen de **valorisation d'une organisation** : due diligence en vue d'une fusion-acquisition[35] ou lors de l'arrivée de nouveaux investisseurs, en évaluant l'exposition aux risques d'une partie prenante.

Au-delà de ces quatre apports de valeur, un retour d'expérience récolté auprès d'acteurs de la notation montre toutefois une frilosité de la part des décideurs à communiquer ces notes à leurs COMEX. Deux raisons au moins sont évoquées. La première est liée à la volonté de se comparer à ses pairs sans chercher à faire mieux qu'eux. Cela installe un plafond de verre budgétaire qui contrarie le principe d'amélioration continue, base d'un SMSI. **S'agirait-il d'une spécificité française de lier les budgets de la sécurité aux incidents plutôt qu'à l'anticipation**[36] ? La seconde raison est liée à la difficulté de faire évoluer la note même pour les organismes les plus matures.

La qualité de la note cyber

Il n'y a pas de norme ou de consensus pour définir une note. Chaque agence propose le résultat de son algorithme maison et l'analyse de ses propres experts. Chacun d'eux pourrait devenir la référence implicite d'un futur standard qu'il finirait par s'imposer à tous. La jeunesse du métier implique toutefois quelques dérives qu'il conviendrait de cadrer d'autant qu'elles imposent parfois des arbitrages desservant l'intégrité recherchée par les experts. Une norme de notation construite autour d'un consensus aurait l'utilité de remettre ces dérives face aux objectifs de notation d'une performance et pas d'une simple conformité *stricto sensu*.

Edgar MORIN nous enseigne qu'une réduction équivaut à une mutilation et une « pensée mutilante conduit nécessairement à des actions mutilantes ».[37]

Les potentiels problèmes de la notation cyber sont :

- Une **qualité de la collecte** d'information différente si l'organisme testé est payeur (et donc client) et non-payeur. Pour pouvoir comparer un organisme payeur à ses concurrents, l'agence doit poser des critères de collecte. Ces discriminants font le socle d'informations traitées par l'algorithme de notation et influent fortement sur le résultat. Un organisme non-payeur peut ainsi se voir affubler d'une mauvaise note liée à un critère qui ne le reflète pas. (exemple : un critère tel que le mot clé «Ariane » nous fera remonter des informations sur la fusée Ariane, le site des affaires étrangères du gouvernement français, ou encore des blogs sur la mythologie). Un client « payeur » pourra lui entamer les discussions pouvant qualifier la surface d'attaque correspondante à sa réalité (celle qu'il souhaite noter) ;

[35] ibid.
[36] Exemple : en 2016, au lendemain de l'attaque Wannacry mettant à terre un nombre important d'entreprises, les serveurs réputés impossibles à mettre à jour depuis des mois, ont tous subit les campagnes de patch requis en une semaine.
[37] Edgar Morin, Introduction à la pensée complexe.

- Une **<u>analyse incomplète</u>** est systématiquement menée. Ceci est causé par un tropisme de collecte OPEN SOURCE qui permet de travailler sur l'empreinte numérique et les vulnérabilités identifiables depuis Internet. Or, toute la complexité et l'efficacité d'un SMSI[38] ne sont pas forcément perçues par ce moyen. Le paradigme de la défense en profondeur autorise l'existence de vulnérabilités à des points bien choisis et acceptés par l'entreprise[39]. L'organisme non-payeur n'ayant pas de relation avec l'agence qui lui attribue une note, ne pourra pas défendre le choix managérial qu'il a fait, sur la base d'une analyse de risque, en équilibrant le gain business, les obligations règlementaires et les mesures de sécurité mises en place ;
- Certaines méthodes de collecte d'information pourraient être frappés d'**illégalité** au regard de la loi n°88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain et la loi n°2004-575 du 21 juin 2004 dite « Loi de Confiance dans l'Économie Numérique ». Les infractions sont potentiellement : le recel d'information[40], l'entrave au bon fonctionnement[41], ou simplement l'accès frauduleux[42]. Plus simplement, sans autorisation explicite, le moindre usage d'outils techniques pour découvrir les caractéristiques du système d'information d'un organisme pourrait facilement tomber dans le périmètre de ces textes. Dans la « vraie vie », l'utilisation de ces outils est tellement courante, pour de bonnes ou de mauvaises raisons, qu'il est impensable d'imaginer des poursuites à chaque occurrence détectée. Il n'existe pas que des outils permettant d'énumérer. D'autres, plus intrusifs, découvrent des erreurs de configuration, souvent simples, mais répandues et surtout efficaces pour un attaquant. L'exemple le plus simple est l'exposition sur Internet d'une interface d'administration ayant l'identifiant et le mot de passe par défaut encore valides. Le simple fait de s'y connecter consciemment sans en avoir l'autorisation est frauduleux, bien que sans aucun impact si aucune autre manipulation n'est faite. Le doute[43] ne porte donc pas sur les organisations ayant contractualisé avec les agences, mais sur les entreprises qui se retrouvent évaluées sans accord préalable, la promesse commerciale étant de pouvoir se comparer à ses pairs. En revanche, il y a peu de doute à avoir sur le respect des lois françaises par une agence notation exerçant sur le territoire français, mais Internet n'ayant pas de frontière, une entreprise basée hors de

[38] Système de management de la sécurité de l'information.
[39] Identifié et évalué par une analyse de risque.
[40] Le recel d'informations obtenues à la suite d'une intrusion frauduleuse dans un système de traitement automatisé de données est puni par l'article 321-1 du Code pénal de cinq ans d'emprisonnement et de 375 000 euros d'amende.
[41] L'article 323-2 du Code pénal incrimine le fait de fausser ou d'entraver le fonctionnement du système informatique. Cela est passible de cinq ans d'emprisonnement et de 75 000 euros d'amende. Peu importe qu'il y ait eu accès – autorisé ou non – au système informatique de la victime, il s'agit ici de réprimer des dégâts causés volontairement aux données et au système, notamment, par exemple, par l'introduction d'un virus. L'envoi massif de courriels non sollicités (ou spamming) est un autre exemple d'entrave au système (CA Paris, 18 déc. 2001, D. 2002, p. 940). En revanche, pour que l'infraction soit constituée, il faut que le fonctionnement du système soit faussé ou entravé, c'est-à dire qu'il soit affecté de manière préjudiciable.
[42] L'accès frauduleux est constitué dès lors qu'une personne non habilitée pénètre dans un système de traitement automatisé de données tout en sachant qu'elle est dépourvue d'autorisation. L'article 323-1 du Code pénal sanctionne la pratique du hacking frauduleux. Il rend les intrusions dans un système de traitement automatisé de données passibles de deux ans d'emprisonnement et de 60 000 euros d'amende..
[43] La méthodologie de collecte et l'algorithme utilisé n'étant au mieux que « partiellement » communiquée.

France sous une juridiction moins contraignante, voir autorisant le hack-back pourrait très bien se jouer (intentionnellement ou non) de la frontière floue qui s'installe entre le monde technique réel et la contrainte légale.

- Un **manque de transparence** sur la méthodologie de notation. Les principes et méthodes menant à la publication d'une note restent dans la plupart des cas propriétaire et ne sont communiqués (intégralement ou partiellement ?) qu'à certains clients, sous couvert d'un NDA[44]. La note produite par ce tiers de confiance étant utilisée également pour rassurer les clients de cet organisme noté, ces derniers devraient pouvoir également en avoir librement et facilement connaissance afin de se conformer à l'adage qui dit : « la confiance n'exclue pas le contrôle ». Ceci pourrait également proposer l'avantage d'être vérifiable par ses pairs avec un double bénéfice. La reproductibilité des analyses qui amènerait de la confiance au départ, et l'application du principe d'amélioration continue qui maintiendrait cette même confiance dans la durée.
- Le **conflit d'intérêts** est également à envisager pour deux raisons. La première est liée au modèle économique émetteur-payeur que l'on retrouve également dans les agences de notation financière. Le rapport du sénat de juin 2012 préconise à ce propos d'imposer un modèle investisseur-payeur. La seconde est propre aux offres de services additionnelles de certains organismes attribuant des notes, ce qui a été interdit pour les agences financières.
- Les **compétences des analystes** sont inconnues. Les phases de collecte et d'analyse sont en grande partie automatisées. Cela n'empêche que pour contextualiser ces résultats et apporter de la valeur (en fonction de la prestation proposée par les agences) la présence de compétences humaines est indispensable, d'autant que certaines agences mettent en avant leur CTI (Cyber Threat Intelligence) pour consolider cette note. Or, pour répondre à la demande actuelle des entreprises, il faudrait plus que doubler le nombre de spécialistes en cyber sécurité. Dans ce contexte de forte concurrence, les agences pourraient n'avoir d'autre choix que de s'appuyer sur des profils trop juniors[45] pour des charges de travail trop importante[46], à l'instar des agences financières. Le manque de certification spécifique aux « agents de notation » l'autoriserait implicitement[47].
- Mal comprise, une bonne note donne un **faux sentiment de sécurité** au COMEX n'aidant pas le directeur de la sécurité de l'information à obtenir le budget nécessaire au maintien de son SMSI (Système de Management de la Sécurité de l'Information). À l'inverse, une mauvaise note orientera les budgets vers un projet permettant de paraître plus sécurisé. **L'effet pervers serait la priorisation de la**

[44] Non disclosure agreement.

[45] 62 % des analystes affectés à la notation des entreprises avaient moins de cinq années d'ancienneté en 2009-2010 et, seulement 14 % des analystes de Fitch au niveau mondial disposaient de la certification externe de « Chartered Financial Analyst ».

[46] « L'analyste note beaucoup trop d'organismes pour que cela soit sérieux, il n'a pas de temps d'approfondir », Interview *« Standard&Poor's, Moody's, Fitch : des agences de notation en roue libre ? »* du 7 février 2019,

[47] La certification PASSI de l'ANSSI ne semble pas adapté à cette activité. L'analyste ne connaît sa proie que par ce qu'il en voit (open source). *Sa note est donc une évaluation en continu* de la posture de cyber protection et de cyber défense d'une organisation telle que vue par les autres.

protection des systèmes informatiques au détriment de de la protection de l'information.

La Cyber notation et l'autonomie stratégique

Globalement, le poids des agences financières et les notes qu'elles attribuent ont une capacité d'influence non négligeable dans le financement des États, des entreprises, des dues diligences, ou de la relation de confiance entre clients et fournisseurs. La convergence des notes financières et de leurs homologues extra-financières vers un système de notation commun renforce cet effet d'où l'importance pour un État ou une entreprise de pouvoir s'appuyer sur une agence qui partage la même communauté de destin et de la même communauté de dessein afin de favoriser l'autonomie stratégique. Cependant pour une organisation européenne cherchant à se faire noter, les agences candidates sont restreintes. Une cartographie des agences qui produisent ces notes, met en évidence une asymétrie, à l'avantage des États-Unis, tant sur le nombre d'acteurs que sur les financements bien supérieurs dont ils disposent, vis-à-vis de leurs homologues européens. Outre les agences spécialisées, les émanations des agences financières (exemple : Moody's qui s'associe au think tank israélien Team8) disposent de la puissance financière ainsi que d'un parc de clients captifs internationaux déjà établi.
Trois familles de producteurs de notes sont identifiables :

- **Les agences de notation financière** qui ajoutent une notation cyber à leur catalogue. Elles reproduisent principalement leur métier d'origine, mêlant analyse d'information open source et audit interne.
- **Les agences de notation spécialisées en cyber** et n'ayant que cette activité, apportent la lisibilité.
- **Les sociétés de service ayant des offres autour du management de risque cyber** et ajoutant une activité de notation. Leur apport est plus centré sur l'expertise technique et l'accompagnement dans l'amélioration continue. Dans ce cas de figure, l'analogie avec le début des agences financières est à remarquer. Ces dernières ont par la suite été sommées de ne pas proposer de services additionnels afin d'éviter les conflits d'intérêts.

Il est à noter que lors du « Forum International de la Cyber sécurité » 2020, seuls Security-scorecard et Bitsight (deux acteurs US) avaient un stand et sont intervenus dans des ateliers publics participant ainsi à l'influence de ces sociétés américaines sur le territoire européen. D'autant que celles-ci bénéficient de capitaux très importants levés auprès d'investisseurs de poids, ce qui est compliquée à réaliser pour nos acteurs EU. AXA et la BNP se sont rapprochées d'acteurs américains.
L'histoire se répétant, tous les indicateurs laissent penser que le cyber-rating pourrait finir à terme et si rien ne s'y oppose, à être délégué à un savoir-faire américain laissant ainsi un vecteur d'influence supplémentaire dans les mains d'une puissance étrangère. La notation est un métier dont la nature est anglo-saxonne à l'instar de la normalisation.

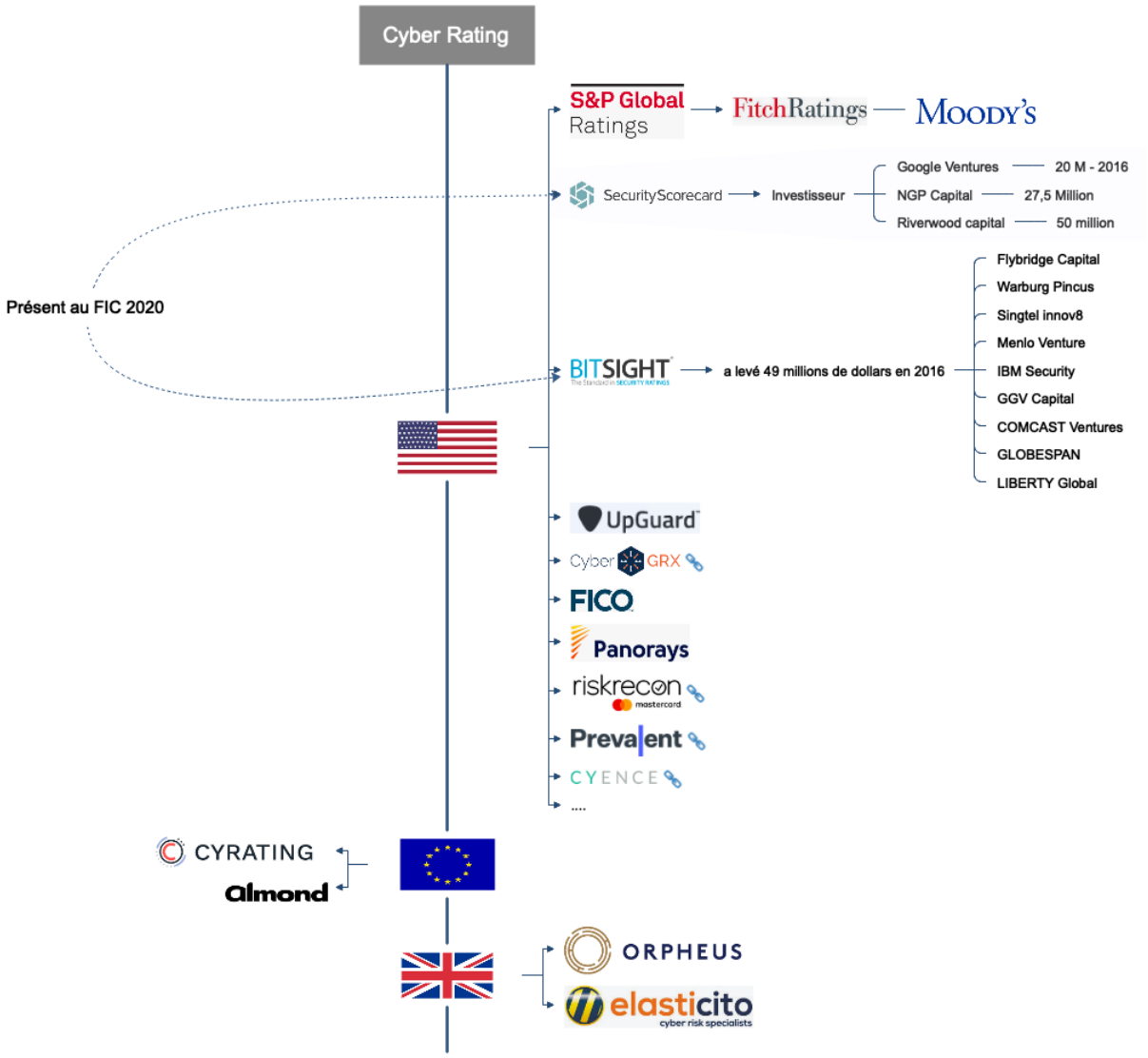

Figure 5: cartographie des agences de notation (non exhaustif)

Comment répondre ?

L'activité du cyber-rating est toujours en recherche de maturité et sans actions rapides pour réguler ce marché, il ne serait pas surprenant d'avoir dans quelques années un rapport du sénat portant sur le risque des agences de notation cyber similaire à celui qui a été déclenché par la crise de 2008 mettant en évidence les carences relevées plus haut.
Pourtant il existe encore des options que nous pourrions explorer pour favoriser des acteurs compatibles avec une autonomie stratégique de l'Europe et des entreprises européennes.
Deux volets sont à prendre en compte :

- Des actions défensives afin de protéger le marché :

- Imposer l'utilisation d'un algorithme d'analyse open source pour plus de transparence et d'équité dans les comparaisons[48] ;
- Créer une certification « d'analyste en notation cyber » ;
- Créer une certification autorisant les agences à collecter les informations techniques (scans) au-delà des textes limitants en vigueur ;
- Interdire l'activité de notation à toutes les agences n'ayant pas obtenu la certification adéquate ;
- Promouvoir le partage d'information avec l'état afin de favoriser l'amélioration de la cyber-sécurité globale au sein d'un territoire.

- Des actions offensives afin de favoriser le business :
  - Imposer l'usage de la notation aux opérateurs d'importance vitale et services essentiels (OIV/OSE).
  - Imposer la souscription à une assurance cyber aux acteurs économiques les plus sensibles.

Jean-Michel BARBIER

Mes remerciements à Clément CHEVIGNON, Laurence BAULT et Mathieu MEYER.

[48] Cet algorithme serait imposé déposé par l'ANSSI qui animerait son amélioration continue avec une communauté du libre. Il serait également un moyen d'inciter à respecter un minimum de « niveau de cybersécurité »