LES ENTREPRISES PILOTES EN MATIERE DE SECURITE GLOBALE : MYTHE OU REALITE ?

Sous la direction de Christian Harbulot

MRSIC 3

MBA Management des Risques, Sûreté Internationale et Cyber Sécurité

École de Guerre Économique

Hamza Benkaïd – Arthur Guiol – Nathalie Kienga – Alexandre Morliere

« Le modèle de sécurité historique de l'entreprise « forteresse assiégée » a vécu et que celui de l'entreprise « hub d'aéroport international » est plus pertinent ».

Jean-Paul Bonnet, Directeur Sûreté de Safran

TABLE DES MATIERES

Table des matières 3
Résumé 5
Introduction 6
La sécurité globale, un concept étatique 7
La genèse du concept de sécurité globale 7
Exemples de concepts de sécurité globale étatique 8
Les Etats-Unis : le Homeland Security 8
La sécurité à la mode chinoise 12
La sécurité globale, le concept en entreprise 16
Définition 16
La sécurité globale : un terme marketing 17
L'organisation de la sécurité des entreprises 18
Le cas français : étude du CDSE 18
La place de l'intelligence économique 21
Le cas des grandes multinationales 23
Un exemple d'organisation en lignes de défense 25
gestion du risque et transferts assuranciels 28
Définition 28
Le traîtement du risque 28
La stratégie de gestion du risque 32
Les enjeux de la cybersécurité pour l'entreprise 34
La genèse de la cybercriminalité 35
Les vecteurs de vulnérabilités de l'entreprise 36
Les typologies de menaces 36
Le facteur humain 37
La pénurie de ressources humaines 38
La gestion des données et le RGPD 38

Les enjeux pour l'entreprise 39
Le coût financier 39
La souveraineté numérique 39
Les coûts de la cybercriminalité dans le monde 41
La cyber-résilience 41
Définition 41
L'illusoire sécurité économique des entreprises 44
Les armes juridiques américaines pour dominer l'économie mondiale 44
L'arme anti-corruption 45
Les sanctions économiques 47
L'hégémonie sur le commerce militaro-industriel 47
Le contrôle des investissements étrangers 48
Le protectionnisme commercial 48
Le Cloud Act 49
Les dépendances économiques 49
Sous l'ombre des États 50
Sous la coupe des cabinets d'avocats d'affaires anglo-saxons 59
Sous le poids des géants du numérique : GAFAM, BATX, NATU 60
Les investissements stratégiques : les fonds vautours 67
Conclusion 70
Bibliographie 71

RESUME

Le concept de sécurité globale appliqué à un État trouve son plus bel exemple dans l'organisation de la sécurité nationale aux États-Unis. Piloté par l'exécutif américain, le « *Homeland Security* » est un enjeu politique et stratégique majeur pour assurer la domination mondiale du pays, notamment sur le plan économique. Mais les États-Unis ne sont pas les seuls à apporter une importance capitale à l'organisation de la sécurité nationale. La Chine fait preuve également d'une redoutable efficacité depuis qu'elle a décidé de devenir la première puissance mondiale.

La mondialisation et la numérisation de l'économie ont également poussé les entreprises à organiser leur sécurité. Si les entreprises de taille moyenne resteront vulnérables du fait du manque de moyens humains et financiers pour apporter une réponse globale à leurs enjeux de sécurité, ce n'est pas le cas des grands groupes qui s'organisent. De la sécurité-sûreté « classiques », les entreprises ont intégré la cybersécurité ainsi que l'intelligence économique dans leur organisation pour protéger les personnes et les biens matériels et immatériels. Mais l'organisation de tous ces métiers dans l'entreprise et la bonne circulation de l'information sont des difficultés très présentes. L'évolution très rapide des risques cyber et la difficulté de prise en compte de l'ensemble du domaine de l'intelligence économique sont des défis que les entreprises peinent à surmonter pour pouvoir prétendre être pilote en matière de sécurité globale.
De plus, les entreprises ne peuvent pas assurer seules leur sécurité économique. En effet, face au patriotisme économique agressif des pays comme les États-Unis ou la Chine, les entreprises subissent les enjeux de puissance et sont les victimes directes des guerres économiques entre États. Les lois extraterritoriales, le protectionnisme ou encore les fonds d'investissements sont autant d'armes de guerre économique face auxquelles les entreprises peuvent difficilement se prémunir sans le soutien d'un État fort.
Il ne faut pas oublier les dépendances créées indirectement par ces États, que ce soient dans les domaines technologique, numérique, énergétique ou encore simplement dans le monde des affaires (cabinets de conseil et d'affaires). Ce sont des risques face auxquels les entreprises dépendantes n'ont pas de solution de protection.

L'organisation de la sécurité des entreprises a fait des progrès considérables au cours des dernières décennies. Aujourd'hui, les grands groupes qui sont « adossés » à un État fort, sont bien protégés. Mais néanmoins, les vulnérabilités sont encore trop grandes pour que ces derniers puissent prétendre maitriser leur sécurité globale. Les entreprises françaises, et notamment celles du CAC 40 restent encore trop vulnérables et dépendantes dans de nombreux domaines.

INTRODUCTION

La sécurité serait-elle la première des libertés… ou peut-être l'inverse ? En tout cas, c'est au nom de la liberté que les États cherchent, au prix d'énormes efforts, à sécuriser leurs espaces (physique et virtuel) contre des dangers multiformes, évolutifs et de plus en plus nombreux.

C'est dans un contexte à grands bouleversements, avec l'apparition de nouvelles menaces, que né le concept de la « sécurité globale », tel que nous tenterons de le définir. Les États doivent être alors en mesure d'avoir la capacité d'assurer une protection efficiente à leur nation pour que cette dernière, en cas d'attaques en tout genre, ne soit pas impactée de manière drastique.

A l'instar des États, les entreprises subissent les évolutions de notre époque, avec les menaces qui les accompagnent. Ainsi, chaque année, des milliers d'entreprises sont victimes d'attaques majeures, principalement des vols d'informations stratégiques, des actes de malveillance ou encore des cyberattaques. Leurs effets sont variables mais les conséquences peuvent être catastrophiques : la moitié de ces entreprises verront leur chiffre d'affaires impacté, pour d'autres, ces attaques leur seront fatales. Ceci est dû au fait que la plupart des entreprises sont mal préparées ou n'anticipent pas les menaces dont elles sont les cibles.

Le monde change et les entreprises sont dans l'obligation de se révolutionner avec lui pour continuer d'exister. Pour faire leur mue, les entreprises doivent être en mesure de réaliser un diagnostic des risques potentiels qui les entourent. Les objectifs sont alors de les anticiper et de préserver leurs capacités à grandir et à innover, mais aussi d'augmenter leur résilience face aux menaces, les rendant ainsi moins vulnérables aux failles qu'elles pourraient avoir.

Nous nous intéresserons dans notre étude à l'organisation de la sécurité/sûreté des entreprises françaises et des grands groupes afin d'évaluer comment elles évoluent pour résister aux nouvelles menaces. Également comment chaque acteur se doit d'être mobilisé pour accélérer la création d'une culture de la sécurité globale, à l'image de ce que réalise déjà certains États, précurseurs en la matière, dont les entreprises sont des concurrentes agressives sur des marchés toujours plus compétitifs.

Dans cette appropriation de la culture de la sécurité globale, la gouvernance et l'organisation joueront un rôle clé, c'est eux qui devront apporter la dynamique nécessaire qui amènera les comportements individuels et collectifs à évoluer afin de renforcer la capacité de résilience de l'entreprise.

Nous verrons que pour éviter une confrontation directe avec un État, l'entreprise est la cible d'attaque de la part d'individu, d'organisation criminelle ou de gouvernement. C'est dans cette optique que nous mettrons en avant qu'une véritable coopération de sécurité public/privé est devenue un enjeu stratégique pour les entreprises. Mais si théoriser cette collaboration est aisée, dans les faits son application reste encore marginale. Seuls quelques États précurseurs, comme les États-Unis et la Chine, mettent en place ce type d'organisation pour prétendre à la sécurité globale de leurs entreprises.

LA SECURITE GLOBALE, UN CONCEPT ETATIQUE

LA GENESE DU CONCEPT DE SECURITE GLOBALE

Dans notre étude, nous abordons le thème de la sécurité globale au sein des entreprises mais pour en trouver son origine et en définir l'expression, il faut remonter à un échelon supérieur : celui de la nation. En effet, il s'agit de la transposition d'une théorie avant tout étatique.

Depuis l'Antiquité, l'Homme a toujours fait de la sécurité l'un des piliers fondamentaux de la nation. Dès lors, à mesure que le monde évoluait, il n'a eu de cesse de s'adapter et se réorganiser face à de nouveaux dangers et nouvelles formes de menaces traduisant de nouveaux défis sécuritaires.

La fin de la guerre froide a rendu les paradigmes classiques qui prédominaient désuets. La fin de ce système bipolaire, l'apparition de nouveaux dangers et la montée de menaces considérées, jusque-là, marginales, comme le salafisme, amènent à repenser la sécurité. C'est à cette période, en 1991 plus précisément, que la notion de sécurité globale apparaît pour la première fois, loin de la vision sectorisée existante.

C'est le développement de nouvelles menaces (liées à la mondialisation, au terrorisme, aux nouvelles technologies, aux catastrophes naturelles,...) mais plus particulièrement, un évènement majeur, celui des attentats du 11 septembre 2001 aux États-Unis, qui rabattent les cartes et qu'un vrai paradigme de la sécurité globale prend forme. Il devient impératif de considérer les différentes menaces dans leur globalité afin d'assurer pleinement la sécurité d'un État et de ses citoyens. La sécurité intérieure et la sécurité extérieure deviennent alors indissociables et interdépendantes.

La sécurité globale « est, au-delà d'un État, la capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles »[1] . Cette définition tend à montrer que la sécurité nationale n'est pas qu'affaire d'État et souligne l'importance et la nécessité d'une étroite collaboration entre les secteurs public et privé dans le cadre de la sécurité globale.

Elle a pour objet la mise en place des mécanismes appropriés et performants pour protéger des infrastructures, une population, un territoire et des frontières. Elle intègre la continuité d'activité, la gestion de crise, une stratégie de réponses aux menaces et une organisation de la résilience.

La sécurité globale recouvre de manière interopérable et transversale différents aspects : la sécurité civile, la sécurité économique, la sécurité juridique, la sécurité informatique et numérique (données, réseaux,…), la sécurité sanitaire (risques biologiques, pandémies, catastrophes naturelles), la sécurité alimentaire, la sécurité du territoire (aérienne et maritime), la sécurité des transports (terre, air et mer), la sécurité industrielle…[2]

[1] Définition de l'Institut National des Hautes Études de la Sécurité et de la Justice (INHESJ)
[2] https://www.diplomatie.gouv.fr/IMG/pdf/PSD_266_Dossier_Reforme.pdf

Après cette présentation générique de la sécurité globale, nous allons aborder brièvement les actions mises en œuvre par les États-Unis et la Chine et comprendre ce qui les ont amenés à repenser leur sécurité de manière drastique et plus globale.

EXEMPLES DE CONCEPTS DE SECURITE GLOBALE ETATIQUE

LES ETATS-UNIS : LE HOMELAND SECURITY

Les attentats du 11 septembre ont été un véritable cataclysme pour les États-Unis et le reste du monde et ce à bien des égards. Sûrement par suffisance, la première puissance mondiale ne s'attendait pas à être attaquée au plein cœur de son sacro-saint sanctuaire, son territoire national, dont elle surestimait la cuirasse. Les États-Unis s'évertuaient, jusqu'à ce moment-là, à défendre essentiellement leurs intérêts en dehors de leurs frontières.

Ces attaques ont mis en lumière les défaillances du système sécuritaire américain, notamment le système informatique dédié à la recherche du renseignement. A partir de là, les États-Unis ont placé la sécurité nationale au cœur leurs préoccupations politiques.

Une première mesure voit rapidement le jour, le USA *Patriot Act*[3], loi antiterroriste votée par le Congrès des États-Unis et signée par George W. Bush, le 26 octobre 2001. Le *Patriot Act* renforce le pouvoir des agences nationales de sécurité et de surveillance, comme la NSA, la CIA, le FBI et aussi de l'armée, dans la lutte contre le terrorisme.

Cette Loi amène à la création de nouveaux statuts juridiques, ceux de « combattant ennemi » et de « combattant illégal », qui permet d'arrêter, d'inculper et de détenir sans durée des personnes soupçonnées de terrorisme, comme ce fut le cas pour les prisonniers de Guantanamo.

Le *Patriot Act* autorise le fait que des perquisitions soient menées et que des saisies de documents et de matériels soient effectuées sans que le suspect ne soit prévenu et sans la présence nécessaire de ce dernier. Des suspects sont également détenus pendant des mois sans toutefois avoir la possibilité d'être défendus par un avocat. Ceux qui ont accès à un avocat voient leurs conversations téléphoniques, avec celui-ci, écoutées. Le *Patriot Act* permet au gouvernement américain d'aller très loin dans la privation de certains droits jusque-là inaliénables.

Les agences gouvernementales sont autorisées à avoir accès aux données numériques des citoyens délivrés par les opérateurs télécoms et ont la capacité de mettre sur écoute et d'exploiter les données recueillies par surveillance électronique sans que les utilisateurs en soient informés. Le *Patriot Act* prévoit que toute intrusion dans un système informatique peut être assimilée à un acte de terrorisme, ce qui vise toute activité de hackers, comme Anonymous, par exemple.

[3] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act,* traduisible en français par « Loi pour unir et renforcer l'Amérique en fournissant les outils appropriés pour déceler et contrer le terrorisme »

Les frontières font l'objet d'une surveillance renforcée, toute personne étrangère arrivant sur le territoire américain doit laisser désormais ses empreintes digitales et sa photographie. Les passeports biométriques sont impératifs.

Ce qui marque profondément la refonte du système sécuritaire américain, c'est la création du Département de la Sécurité intérieure (DHS) des États-Unis[4], créé le 25 novembre 2002, par le *Homeland Security Act*[5] à l'initiative du président George W. Bush. La création de ce département a entraîné la plus importante réorganisation bureaucratique que les États-Unis aient connue depuis la création du Département de la Défense en 1947[6].

D'ailleurs, les diagrammes ci-après montrent bien les répercussions de la création du DHS sur la répartition des financements de la sécurité intérieure entre les ministères concernés. 51% des financements sont alloués au DHS.

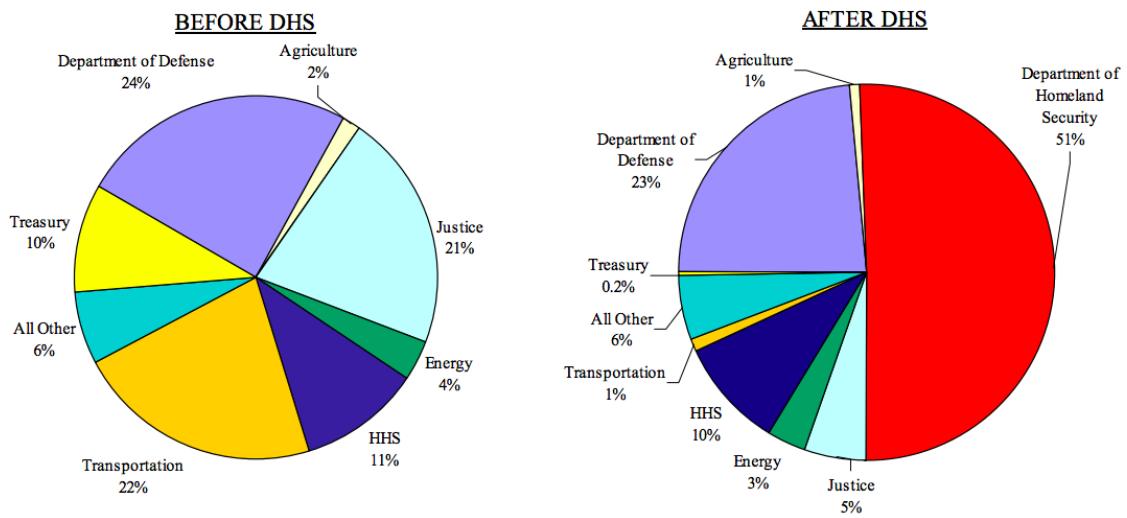


Figure 1 : Evolution de la répartition des finacements de la sécurité intérieure avant et après le DHS

Source : Report to Congress on Combating, 2003

Aujourd'hui, avec un budget de 47,5 milliards de dollars en 2019[7] et plus de 240 000 employés[8], le DHS est le troisième plus grand département américain après ceux de la Défense et des Anciens Combattants.

L'objectif est de centraliser les diverses agences compétentes en matière de sécurité du territoire national en un seul cabinet gouvernemental, d'organiser et d'assurer la sécurité intérieure du pays. Ainsi, le DHS s'appuie sur 22 agences fédérales pour la collecte et le traitement de l'information, notamment la *Cybersecurity and Infrastructure Security Agency* (CISA) pour la protection des infrastructures critiques face aux menaces physiques et cybernétiques, la *United States Coast Guard*, la douane (CBP), le *Secret Service*, les gardes-frontières, l'Agence fédérale des situations d'urgence ou encore l'Administration de sécurité du transport.

[4] En anglais, « United States Department of Homeland Security » (DHS)
[5] En français, « Loi sur la sécurité intérieure »
[6] https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/legislative/2003_combat_terr.pdf Page 6
[7] https://www.dhs.gov/sites/default/files/publications/DHS BIB 2019.pdf
[8] https://www.dhs.gov/about-dhs

Tout comme, le CIA, la NSA et le FBI avec qui il collabore, le DHS s'est vu octroyé de larges pouvoirs par le *Patriot Act*.

Le DHS a la lourde tâche d'éviter toute attaque ou catastrophe susceptible de bouleverser la sécurité sur le sol américain mais également sur les territoires extérieurs où demeurent des intérêts américains.

Ses missions[9,10] sont diverses et variées, le DHS doit :

- Prévenir le terrorisme et renforcer la sécurité sur territoire national.
- Sécuriser et contrôler les frontières aériennes, terrestres et maritimes du pays pour empêcher toute activité illégale tout en facilitant les déplacements et le commerce licites.
- Surveiller et contrôler les communications et les réseaux d'information afin de détecter tout renseignement susceptible de mettre au jour une menace contre le territoire américain.
- Protéger, sécuriser le cyberespace (infrastructures critiques et les systèmes d'information), analyser et réduire les menaces avec l'aide de l'industrie, des gouvernements fédéraux et locaux.
- Appliquer et faire respecter les lois sur l'immigration (application efficace des lois américaines en matière d'immigration, tout en rationalisant et en facilitant le processus d'immigration légale).
- Assurer la résilience aux catastrophes, fournir une réponse globale et coordonnée en cas d'attaque terroriste, de catastrophe naturelle ou autre situation d'urgence de grande ampleur, en collaborant avec les pouvoirs publics fédéraux, les États, et les autorités locales, les partenaires du secteur privé afin de garantir un effort de rétablissement rapide et efficace.
- Prévenir les catastrophes (risque nucléaire, bactériologique, radiologique ou chimique) et prévoir d'éventuelles mesures d'urgence.
- Contribuer à la recherche et au développement de laboratoires universitaires ou d'entreprises, à la pointe de l'innovation sur la prévention des risques terroristes.

La politique du DHS est coordonnée par la Maison Blanche au travers du Conseil de sécurité intérieure (HSC). L'objectif du HSC est d'assurer la coordination de toutes les activités des ministères et des agences liés à la sécurité intérieure, de promouvoir l'élaboration et la mise en œuvre effectives de toutes les politiques de sécurité intérieure. Il réunit statutairement, les hommes situés au plus sommet de l'État, à savoir, le vice-président, le secrétaire d'État, le secrétaire du Trésor, le secrétaire de la Défense, le procureur général, le secrétaire à l'Énergie, le secrétaire de la Sécurité intérieure, le conseiller à la Sécurité nationale, le conseiller à la Sécurité intérieure et l'ambassadeur aux Nations Unies autour du président. Celui-ci le préside, tandis que son administration est dirigée par le conseiller à la Sécurité intérieure.

La structure centralisée de cette organisation montre, encore une fois, à quel point la sécurité intérieure est primordiale et fondamentale aux yeux des États-Unis, puisqu'aucune décision en la matière n'est actée sans l'aval du président et d'un noyau très restreint d'hommes aux plus hautes fonctions.

[9] https://www.dhs.gov/mission
[10] http://www.assemblee-nationale.fr/12/pdf/rap-info/i1664.pdf

Le DHS est l'instrument souhaité par l'État américain pour répondre de manière globale aux problématiques de sécurité intérieure et extérieure dont les États-Unis pourraient avoir à faire face en permettant, d'une part, la collaboration de l'ensemble des forces compétentes américaines en matière de sécurité et d'autre part, en sollicitant la participation d'acteurs issus de la société civile capables d'apporter leur contribution pour la protection de l'ensemble de nation et ses intérêts. Ainsi ce mastodonte de la sécurité, avec son architecture au maillage serré et complexe, permet d'améliorer et de simplifier la communication et le partage d'informations entre les agences elles-mêmes, les autres organisations et les entreprises du secteur privé.

Si auparavant la sécurité nationale relevait essentiellement des agences fédérales, avec le *Homeland Security Act*, le gouvernement n'étant pas en mesure de tout assumer seul, la responsabilité devient partagée avec les gouvernements des États, les collectivités locales et surtout le secteur privé qui participe à « l'effort de guerre ».

Cette collaboration entre l'État et les entreprises privées est facilitée par le fort esprit patriotique qui anime les américains mais surtout parce que plus de 85% des infrastructures critiques sont détenues et exploitées par le secteur privé[11] qui les maitrise mieux que quiconque. L'État se sert alors de l'expertise et des compétences des acteurs privés pour gérer au mieux ces infrastructures, se tourne même vers le secteur privé pour former des partenariats destinés à protéger les infrastructures nationales vitales. Un échange collaboratif se met en place : les entreprises privées transmettent leurs connaissances aux différentes agences gouvernementales concernées et le DHS se charge d'alerter les tiers privés en cas d'alertes de menaces. Ce partage d'informations pertinentes entre les secteurs public et privé permet à chacun de trouver ses propres intérêts au profit de ceux de la nation toute entière.

Mais cette synergie des forces ne s'est pas simplement limitée à la défense du territoire national. Comme l'indique Ali Laïdi, docteur en sciences politiques, spécialiste de l'intelligence économique et chercheur à l'Iris, les attentats du 11 septembre 2001 ont été un « vrai point de rupture », ce sont eux « qui ont révélé à l'Amérique les liens incestueux entre corruption, argent sale et terrorisme »[12]. Et si le *Patriot Act* a été initialement créé pour lutter contre ce système menaçant la pérennité des États-Unis, il s'est rapidement musclé grâce à des lois et des décrets déjà existants ou créés durant la période par le gouvernement américain dans l'intérêt même des États-Unis. L'utilisation de ses lois et décrets a eu pour but d'élargir le spectre d'action du DHS et plus globalement du gouvernement américain afin, non plus de se défendre seulement contre un ennemi invisible mais aussi d'attaquer quiconque s'en prendrait aux intérêts de l'État et des entreprises américaines que ce soit des États, des organisations ou des entreprises étrangers (voir partie « l'illusoire sécurité économique des entreprises »).

Avec le *Patriot Act,* l'exécutif américain souhaite montrer au reste du monde que, suite aux attentats, ils ont été touchés mais pas coulés et ont l'ambitieux projet de remettre les États-Unis au centre du planisphère. Ceci n'est pas sans rappeler le slogan utilisé par la président américain Woodrow Wilson[13] lors de sa campagne pour sa réélection en 1916 : « *America first* », formule remise au goût du jour et réutilisée par le président Donald Trump, le 20 janvier

[11] http://www.leppm.enap.ca/leppm/docs/Rapports_securite/Rapport10_sécurité.pdf
[12] Ali Laïdi, « Le Droit, nouvelle arme de guerre économique » aux éditions Actes Sud, 2019
[13] 28ème président des États-Unis, élu pour deux mandats consécutifs de 1913 à 1921

2017, lors son discours d'investiture. Pour lui, cela sera l'Amérique d'abord, sous n'importe quel prétexte et à n'importe quel prix.

C'est ainsi, qu'au nom d'une lutte contre la corruption, le gouvernement états-unien s'est lancé dans une guerre économique contre des entreprises stratégiques étrangères en cherchant à les agresser et les affaiblir pour permettre aux entreprises concurrentes américaines de mieux se positionner sur les marchés mondiaux.

Les États-Unis ont fait rentrer le monde dans une guerre 2.0 avec comme arme de destruction massive, le droit américain. Nous montrerons, dans la suite de notre étude, comment la loi de l'extraterritorialité et le *Cloud Act* ont permis l'extension et l'intervention de la justice américaine en pays étrangers.

La sécurité globale telle que l'entend les États-Unis n'est plus simplement d'anticiper et de se prémunir d'éventuelles attaques mais bien d'attaquer avant d'être attaqués dans l'intérêt du pays et de ses entreprises. Sous prétexte de sa sécurité nationale, l'Amérique est prête à bafouer les règles et les lois internationales, se moquant allègrement des éventuelles sanctions qui pourraient être menées contre elle par une communauté internationale somme toute, pour le moment, impuissante face à cette déferlante.

Les États-Unis ont fait de cette coopération privilégiée public/privé une véritable force, eux qui craignent par-dessus toute la fin de la domination du dollar, l'ascension irrésistible du « péril jaune » et l'arrivée de nouveaux concurrents émergents. Mais en attendant, tant que « l'étalon-dollar » subsistera, l'Amérique continuera d'imposer sa loi au reste du monde, fera briller son économie et en fera bénéficier aux entreprises américaines.

Cette forme d'alliance entre État et entreprises nationales n'est pas une spécificité américaine, nous verrons par la suite que la Chine a une vision similaire de sa sécurité globale, au nom de laquelle l'État et les entreprises chinoises se doivent mutuelle assistance. Un extrait de la loi sur le renseignement adoptée par les chinois en 2017 le met parfaitement en valeur : « Toute organisation ou citoyen doit, dans le respect de la loi, soutenir, donner assistance et coopérer avec le renseignement national et maintenir le secret sur toute activité de renseignement dont il a connaissance ».

LA SECURITE A LA MODE CHINOISE

La sécurité nationale de la Chine comprend la coordination de diverses organisations, y compris des agences de maintien de l'ordre, des forces armées, des paramilitaires, des agences gouvernementales et des services de renseignement, dont le but est de protéger la sécurité nationale de la Chine.[14]

Quel contexte pour la Chine ?

L'Empire du Milieu présente un ensemble unique de défis et d'opportunités pour la gouvernance mondiale, le développement économique, ainsi que pour la sécurité et la stabilité, qui ont un impact sur l'Europe et la communauté internationale au sens large.[15]

[14] https://en.wikipedia.org/wiki/National_security_of_China
[15] https://www.sipri.org/research/conflict-and-peace/asia/china-and-global-security

Un point sur la souveraineté numérique de l'Empire

La position historique de la Chine est sans ambiguïté, pour l'Empire, la cyber souveraineté doit dominer l'Internet mondial. Ainsi, le président XI déclarait *"Aucun pays ne peut atteindre la sécurité absolue sans la sécurité globale du cyberespace international"* et par cette allocution nous comprenons bien la position stratégique de la Chine dans la dynamique de contrôle de son réseau.

Le Grand Firewall de Chine, dénommé par analogie avec la Grande Muraille de Chine, est le nom usuel du projet bouclier doré, un projet de surveillance et de censure d'Internet géré par le ministère de la Sécurité publique de la république populaire de Chine. Le projet a débuté en 1998 et a commencé ses activités en novembre 2003. Il agit notamment par blocage d'adresse IP, filtre DNS et URL.[16]

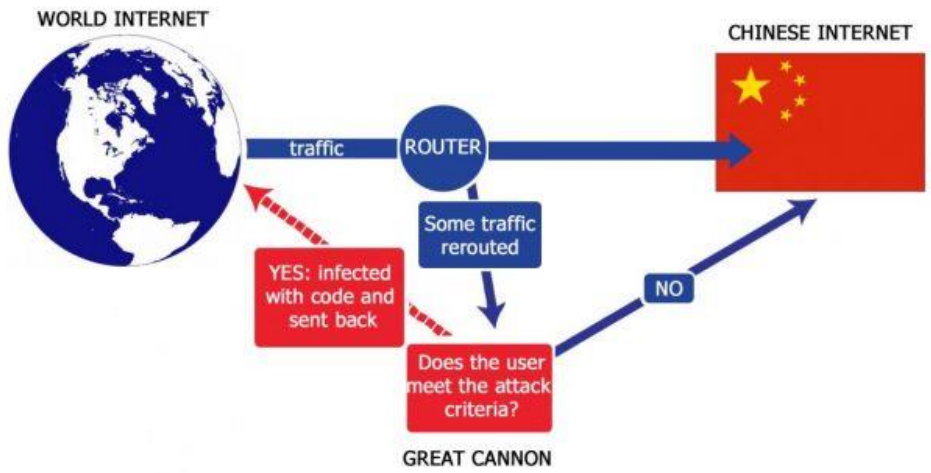


Figure 2 : Le « Grand Firewall » chinois

L'Empire a donc le pouvoir de contrôler l'ensemble de son réseau et n'est absolument pas interdépendant des autres pays du monde au sujet de son trafic numérique.

L'organe de l'État en charge de la sécurité globale

En Chine, il s'appelle le Guoanbu., et c'est le Ministère de la Sécurité de l'Etat (MSE) ou bien *Ministry of State Security (MSS) en anglais* qui est en charge des questions de sécurité globale. Il est l'autorité gérant le contre-espionnage, y compris militaire, le renseignement extérieur, les gardes-frontières, la lutte contre les opposants politiques.

En 2005, un rapport français indique que ce ministère compterait 7 000 fonctionnaires officiels auxquels s'ajoutent 50 000 agents illégaux, les chen diyu (poissons d'eau profonde) dont seulement 150 sont identifiés. Dans le domaine du renseignement économique, les États-Unis sont la cible principale et on compterait dans ce pays 1 500 diplomates opérant dans 70

[16] https://fr.wikipedia.org/wiki/Grand_Firewall_de_Chine

bureaux. Les représentants américains s'inquiètent d'ailleurs ouvertement dans le rapport Cox de l'espionnage Chinois dans leur pays.

Le ministère est divisé en une douzaine de bureaux dont quatre s'occupent entre autres de la guerre économique.

- Le 1er bureau (bureau national) recrute en Chine toutes les personnes se rendant à l'étranger pour études ou affaires.
- Le 2e bureau (bureau étranger) est chargé des opérations à l'étranger : collecte, réception, analyse de l'information, recrutement d'agents à l'étranger et il s'occupe aussi du contre-espionnage.
- Le 10e bureau s'occupe plus spécifiquement des collectes d'informations scientifiques et technologiques.
- Le 17e bureau gère la récolte du renseignement économique, à noter que d'autres spécialistes n'attribuent pas les mêmes numéros aux bureaux selon leur spécialité.[17]

L'une des certitudes concernant le MSE est qu'en Chine, gouvernement, milliardaires, universitaires, citoyens et entrepreneurs travaillent ensemble, en partie parce que l'État exerce un contrôle drastique sur leur vie. Même les géants du secteur privé tels qu'Alibaba, Tencent ou Huawei se trouvent sous pression, l'État-Parti jouant un rôle fondamental pour favoriser, ou entraver, le succès des entreprises, exigeant un droit de regard accru sur leurs activités.

Pour Beijing, la sécurité nationale est l'affaire de tous – Sensibilisation et formation

De récentes lois sur la sécurité nationale ont conféré des pouvoirs sans précédent au Guoanbu. La loi sur le renseignement de 2017 oblige ainsi les entreprises et les citoyens à « coopérer, soutenir ou assister les institutions nationales du renseignement ». En d'autres termes, ils doivent collaborer dans d'éventuelles opérations d'espionnage. Une journée par an, le 15 avril, est même destinée depuis 2016 à sensibiliser les citoyens aux questions d'espionnage et à les encourager à signaler toute activité suspecte.[18]

L'événement a attiré l'attention des médias internationaux, en grande partie grâce à une campagne d'affiches de propagande de Pékin intitulée « *Dangerous Love* ». Dans la campagne, une jeune femme nommée Xiao Li, qui travaille dans la fonction publique, devient amoureux de David, un étranger stéréotypé. David oblige Xiao Li à partager des communications d'État confidentielles afin de soutenir ses « recherches universitaires ». Malheureusement, Xiao Li se trouve bientôt arrêtée et accusée d'avoir révélé des secrets d'État à David, que le gouvernement accuse d'être un espion étranger.

Outre les avertissements évidents adressés aux citoyens chinois, la campagne pourrait mettre les étrangers en garde contre les risques de détention et de discrimination en Chine - en particulier les employés d'ONG ou les chercheurs travaillant sur des sujets sensibles. En effet, la Chine sous Xi Jinping fait en sorte que les étrangers se sentent moins bien accueillis. Cependant, même si de telles interprétations sont véridiques, d'autres facteurs devraient éclairer notre analyse.

La Journée de la sécurité de l'État vise principalement à sensibiliser les masses à la sécurité de l'État et à leur faire prendre conscience de leur responsabilité de participer à sa

[18] https://www.letemps.ch/monde/guoanbu-puissance-renseignement-chinois

préservation. Cela met en évidence une idée du concept de sécurité d'État chinois largement sous-estimée dans les analyses existantes : chaque membre de la société chinoise a la responsabilité de défendre la sécurité de l'État-parti chinois. Pour comprendre cela, il faut garder à l'esprit que la stratégie de sécurité de l'État chinois vise fondamentalement à défendre les dirigeants du Parti communiste chinois.

Comme le parti l'a expliqué à de nombreuses reprises, le concept de sécurité "globale" de la Chine, outre la connotation occidentale de "sécurité nationale", englobe la sécurité politique, la sécurité intérieure, la sécurité militaire, la sécurité économique, la sécurité culturelle culture sanctionnée), la sécurité sociale (impliquant la stabilité sociale) et la sécurité de l'information. Dans l'élaboration officielle du concept de « sécurité de l'État », l'accent est mis sur les questions de préservation entre le Parti et l'État.

À l'échelle nationale, la politique de sécurité de l'État de la Chine est étroitement liée au processus de « gouvernance sociale » ou de « gestion sociale » du PCC. La gestion sociale est le processus par lequel les dirigeants du PCC tentent de gérer leurs relations à la fois avec les cadres du parti et avec la société, afin de s'assurer qu'il reste l'autorité suprême au pouvoir. Pour que le processus fonctionne, la direction du parti et les citoyens sont une exigence essentielle sur laquelle le leadership du parti central s'appuie. Le concept de responsabilité individuelle est inscrit dans la loi de 2015 sur la sécurité de l'État, l'article 11 énonçant simplement : « Citoyens de la République populaire de Chine, tous les organes de l'État et les forces armées, chaque parti politique, la milice, les entreprises, les institutions publiques et les organisations sociales ont tous la responsabilité et l'obligation de maintenir la sécurité de l'État ».

Sur le plan théorique, comme l'a expliqué Xi Jinping à l'occasion de la Journée de la sécurité de l'État, cela signifie que le parti et les masses doivent défendre et développer le socialisme aux caractéristiques chinoises. Ce n'est pas une nouveauté dans la gouvernance de la Chine, mais plutôt une amélioration continue. Comme le suggère la campagne « Dangerous Love », ce processus inclut les étrangers. Le renforcement de la sensibilisation à la sécurité de l'État permettra à la Chine dirigée par le Parti communiste de naviguer dans un environnement de sécurité toujours complexe et incertain.[19]

Le rôle de l'État dans l'éducation, la formation et la sensibilisation à ces questions de sécurité est l'un des plus actif aujourd'hui. Le défi fondamental auquel le parti est toujours confronté pour assurer la sécurité de l'État est que son environnement de sécurité change constamment. Le but des tactiques de préservation de la sécurité de l'État, comme le processus de gestion sociale, est de façonner et de contrôler la société et les cadres du parti à tous les niveaux pour que ces menaces soient plus faciles à gérer.

La vision de la Chine concernant le concept de sécurité globale est tout à fait cohérente. Pleinement consciente des enjeux, de la guerre économique... l'Empire du Milieu est surement l'un des pays les plus matures au monde dans le domaine.

[19] https://nationalinterest.org/feature/dangerous-love-chinas-all-encompassing-security-vision-16239

LA SECURITE GLOBALE, LE CONCEPT EN ENTREPRISE

DEFINITION

Nous avons vu que le concept de sécurité globale s'est d'abord appliqué aux États comme la réponse stratégique aux menaces qui pesaient sur leur « sécurité nationale ». Cela s'est amplifié après la fin d'un monde bipolaire puis l'avènement de la mondialisation, du terrorisme international et de la transformation digitale des sociétés. On constate que pour les États, les définitions divergent, les organisations sont multiples et surtout les périmètres et la finalité du concept sont liés aux ambitions de suprématies de ces derniers.

Le monde de l'entreprise a lui aussi vu se développer les risques liés à cette mondialisation, au terrorisme ou encore à la numérisation. Comme pour les États, ces menaces ont obligé les entreprises à étoffer les métiers liés à leur sûreté/sécurité.

On peut développer une liste non-exhaustive de métiers ou domaines qui couvre :

- La sûreté au sens de la lutte contre la malveillance (vandalisme, sabotage, vol, fraude, terrorisme,…).
- La sécurité au sens de la lutte contre les accidents (incendies, catastrophes naturelles, risques industriels,…).
- La sécurité des systèmes d'information et du patrimoine immatériel (cybersécurité, réputation, protection des données,…).
- La sécurité économique (intelligence économique, droit, protection de l'information, stratégie,…).

Aujourd'hui, tous ces métiers ont pour but de protéger globalement l'entreprise des risques qui pourraient menacer sa pérennité et son développement dans la compétition économique internationale.

Pour l'entreprise mondialisée, le concept de sécurité globale peut se définir ainsi :

> *Protection des personnes et des biens matériels et immatériels, dans un cadre réglementaire et déontologique.*

Si cette définition du concept semble simple et cohérente, nous allons voir que les difficultés résident dans la diversité des expertises nécessaires pour couvrir l'ensemble du périmètre et donc des moyens humains et financiers qui y sont alloués au sein de l'entreprise.

LA SECURITE GLOBALE : UN TERME MARKETING

Très à la mode, le terme de sécurité globale est souvent utilisé à des fins de marketing.

Premier exemple, les prestataires du secteur regroupent sous ce terme des prestations globales de sûreté classique (surveillance humaine et électronique) et de sécurité incendie comme argument de vente.
Quelques-uns y ajoutent des prestations de conseils, de sûreté à l'international, mais très rares sont ceux qui proposent également toutes les prestations de cyber sécurité et d'intelligence économique. De même, de nombreux prestataires de sécurité de systèmes de l'information proposent des offres dites de sécurité globale mais qui couvrent uniquement les risques cyber.
En France, on note un rapprochement de certains prestataires afin de fournir une offre plus globale pour les entreprises, notamment ceux spécialisés dans la sécurité/sûreté privée à l'international et les cabinets spécialisés dans le conseil en intelligence économique/stratégique. L'objectif (au-delà de la survie économique) est de répondre à la demande croissante de leurs clients qui ont besoin de solutions de sécurité de plus en plus globales au sens de notre définition.
C'est le cas de l'ADIT qui a récemment racheté la société GEOS[20,21], mais on peut aussi évoquer la récente alliance entre ANTICIP et le cabinet CEIS, sans oublier le groupe Risk&Co qui pourrait rejoindre cette alliance. Il faut créer des entreprises dont les capacités (économiques mais également opérationnelles) permettent de répondre aux appels d'offre des entreprises mondialisées et des institutions internationales, ce qui n'était pas le cas récemment.

La France essaye de rattraper son retard face aux anglo-saxons, chez lesquels il existe déjà des sociétés qui peuvent fournir des prestations plus complètes, comme par exemple le groupe ControlRisks. Néanmoins, on s'aperçoit que ces prestataires de services ne sont pas encore dimensionnés pour couvrir deux fonctions essentielles de la sécurité globale (sans passer par des sous-traitants) :

- D'un point de vue géographique, l'accompagnement (risques sûreté et intelligence économique) des entreprises dans tous les pays et aussi dans tous les secteurs d'activité.
- La cybersécurité qui reste un domaine de plus en plus technique, que ces entreprises ne maitrisent pas complétement de façon autonome (aucune de ces entreprises n'est aujourd'hui certifiée par l'ANSII).

Si dans certains domaines, l'entreprise peut externaliser tout ou partie de ses problématiques de sécurité, il est pour l'instant difficile de trouver un (ou plusieurs prestataires) qui couvrent l'ensemble du périmètre, sans parler des problèmes de confidentialité. Surtout, il est impératif de garder au sein de l'entreprise une direction sûreté-sécurité pour piloter correctement ces prestations.

C'est cette organisation que nous allons détailler dans les parties suivantes.

[20] https://www.lesechos.fr/industrie-services/air-defense/surete-les-fusions-acquisitions-en-pleine-effervescence du 11/04/2019
[21] https://www.lesechos.fr/finance-marches/ma/nouvelle-alliance-dans-la-surete du 13/06/2019

L'ORGANISATION DE LA SECURITE DES ENTREPRISES

LE CAS FRANÇAIS : ETUDE DU CDSE

Créé il y a plus de 30 ans, le Club des Directeurs de Sécurité et de Sûreté des Entreprises (CDSE) est une association loi de 1901 rassemblant plus de 110 entreprises européennes et aussi des institutions publiques. La majorité des entreprises du CAC 40 y sont représentées par leur direction sûreté-sécurité.

Le CDSE a donc vu évoluer la fonction sûreté-sécurité au sein des entreprises et a également décrit cette évolution au travers de sa revue « sécurité et stratégie » publiée annuellement.

Dans le numéro 30 (octobre 2018) de cette revue, l'article « les enjeux sécuritaires de l'entreprise mondialisée », Franck Vidallo (Promotion EGE SIE 22) revient sur cette évolution et en tire quelques conclusions :

- La globalisation et la digitalisation des entreprises entrainent une dématérialisation croissante des actifs à protéger avec l'émergence de nouvelles vulnérabilités immatérielles.
- L'extraterritorialité du droit comme « nouvelle » menace pour la sécurité économique.
- La pertinence de l'intelligence économique pour répondre à ces nouvelles menaces afin d'avoir une approche globale de la sécurité de l'entreprise.

On est donc loin du temps où la direction sûreté-sécurité (DSS) d'une entreprise était composée du seul directeur sécurité, au budget et aux responsabilités limités à la protection physique des personnes et des biens. Les DSS voient progressivement leurs responsabilités et leurs champs de compétences s'élargir à toutes les menaces qui pèsent sur l'entreprise mondialisée et tendre vers une « sécurité globale », en ajoutant à leur périmètre :

- Les fraudes.
- La sûreté à l'internationale et le risque terroriste.
- La cybersécurité.
- L'intelligence économique.

C'est dans ce sens que le CDSE a mené en 2018 une étude (déclarative, nous y reviendrons) auprès de ses adhérents, dans le but de dresser un panorama de la filière et des métiers de la sûreté-sécurité rencontrés en entreprise, à un niveau *corporate*.

L'étude classe l'organisation des 12 métiers/compétences rencontrés en quatre modules/niveaux :

1. Gouvernance – Pilotage.
2. Expertise – conseil – déploiement.
3. Veille – analyse – suivi.
4. Activités opérationnelles, qui sortent du cadre de l'étude car non considérées comme *corporate.*

Détaillé dans le schéma ci-dessous, ces 12 métiers/compétences couvrent théoriquement l'ensemble des besoins de l'entreprise (et d'une DSS) pour tendre vers une « sécurité globale » :

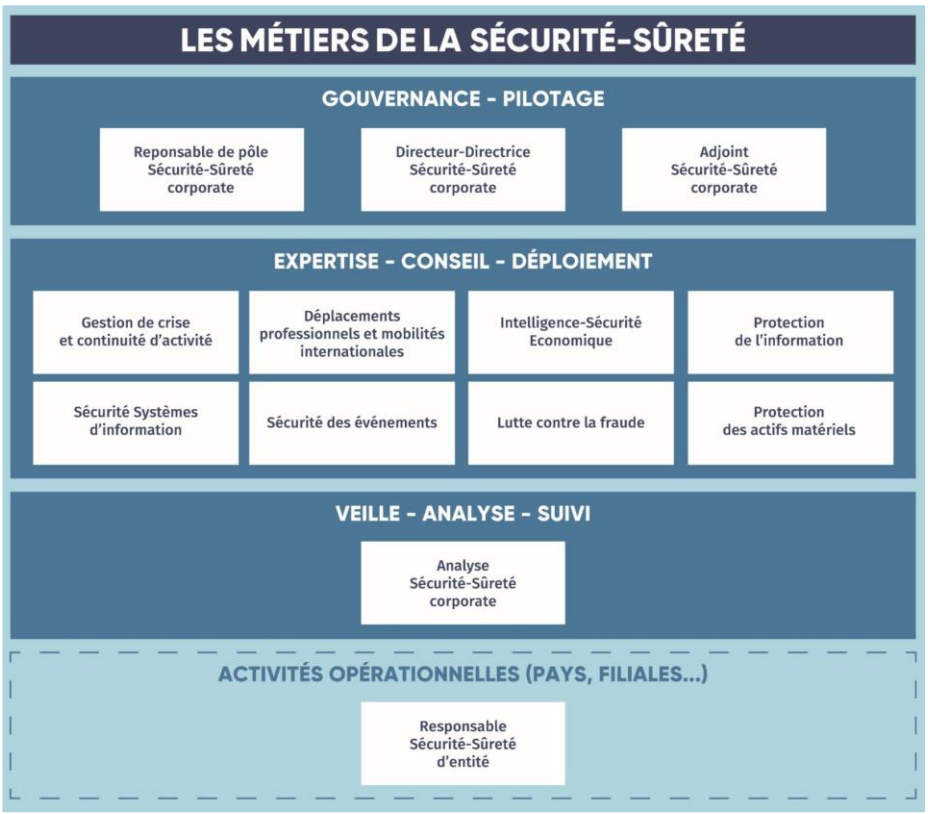


Figure 3 : Étude CDSE "La filière sécurité-sûreté corporate" 2019, les 12 métiers de la filière

Le constat que le CDSE a tiré de cette étude sur l'organisation de la fonction sûreté-sécurité des entreprises est le suivant :

- La fonction évolue vers un positionnement d'anticipation, de prévention, de protection et de création de valeur, en véritable partenaire business (sans préciser le niveau d'évolution).
- Elle multiplie les interactions et doit adapter son positionnement vis-à-vis des autres directions de l'entreprise.
- Dans 74 % des cas, elle est rattachée à la direction générale ou au secrétariat général, ce qui est le niveau « recommandé » pour une gouvernance efficace de la fonction.
- Pour attirer et fidéliser les futurs talents, la filière doit construire des parcours de carrières et accentuer la féminisation de ses métiers.

Enseignement 1 :

Voulue par le CDSE, cette présentation en modules permet de ne pas préciser la structuration des liens hiérarchiques et/ou fonctionnels des DSS selon les spécificités organisationnelles des entreprises. Ceci traduit le fait que les DSS ont des organisations et périmètres différents, de par la taille de l'entreprise, son cœur de métier, sa culture et sa maturité dans le domaine.

Il ne se dégage pas d'organisation type d'une DSS, bien au contraire.

L'étude insiste également sur la transversalité des métiers/fonctions au travers du schéma suivant :

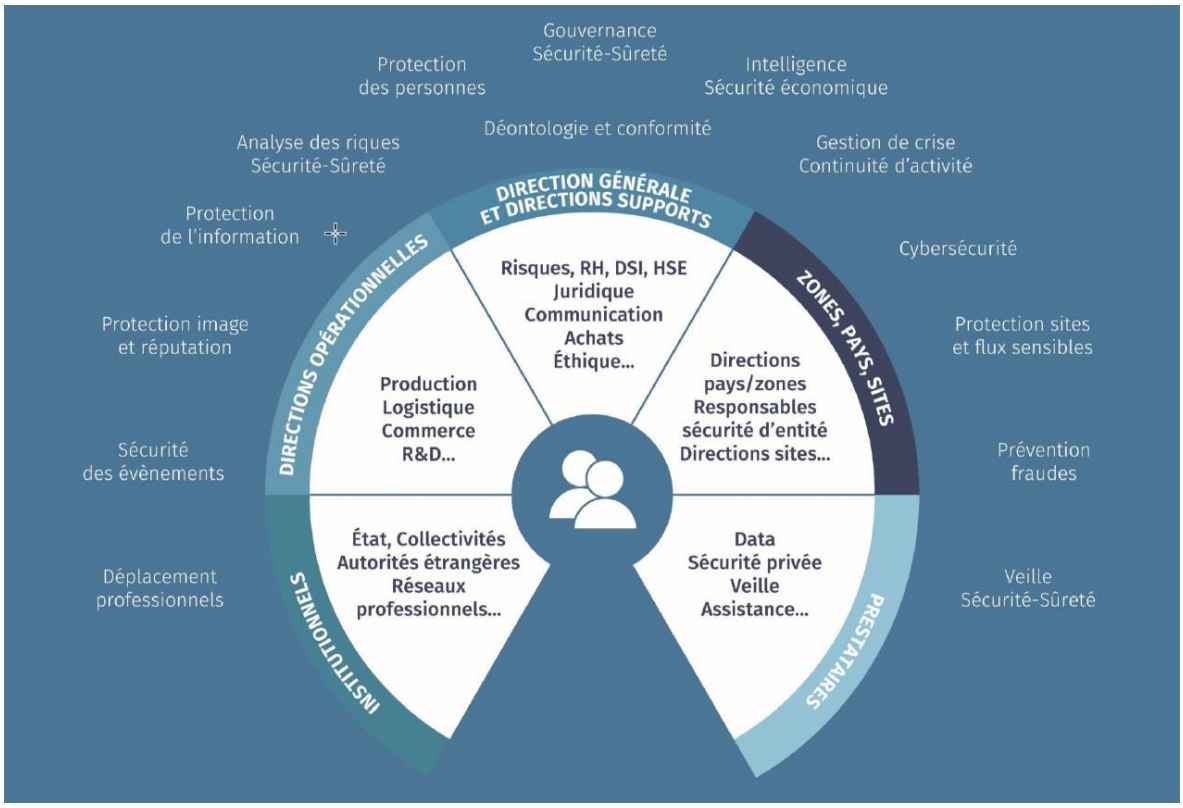


Figure 4 : Étude CDSE "La filière sécurité-sûreté corporate" 2019, transversalité des fonctions sûreté-sécurité.

Il illustre les constats faits par le CDSE :

- La dimension transversale des 12 métiers/compétences qui suppose une connaissance profonde de l'entreprise et des parties prenantes (filiales, partenaires, prestataires,…).
- Le nécessité du concept de « *security by design* » : le besoin d'intégrer les processus sûreté-sécurité dans le système de management et de projet de l'entreprise.
- La variété des postures de la DSS dans les projets : responsables, décideurs, prescripteurs, contributeurs, donneurs d'ordres, conseillers… en lien avec la dimension transverse des métiers/compétences.

Au travers de l'étude, la conclusion du CDSE est ambitieuse pour l'entreprise et les DSS :

- La diversification des menaces et des risques (cyber, terroristes, géopolitiques, juridiques), impose que les enjeux de sûreté-sécurité soient intégrés pleinement à la stratégie de l'entreprise.
- Pour assurer la « sécurité globale » de plus en plus complexe, la filière sûreté-sécurité doit se consolider (moyens humains et financiers) mais également savoir « se vendre » et rayonner au sein de l'entreprise.

Enseignement 2 :

C'est la limite du principe déclaratif de l'étude : les déclarants étant les DSS, elles ne sont pas les plus objectives pour parler de leurs organisations et périmètres. En effet, les DSS n'échappent aux problématiques de positionnement et de structuration au sein de l'entreprise (avec les enjeux de *reportings* et de budgets liés aux périmètres). Ce sont des points essentiels de l'efficacité d'une DSS et plus largement pour une entreprise qui veut prétendre maîtriser sa « sécurité globale ».

De même, l'étude ne précise pas combien de DSS se retrouvent avec des responsabilités qui ne sont pas directement liées au cœur de métier et qui peuvent nuire à leur efficacité en les privant de ressources et de temps. En effet, de nombreux responsables de DSS se voient confier directement la direction d'autres services du type « services généraux » ou « santé-sécurité » (QHSE) avec des problématiques de maintenance, de travaux, d'achats ou encore de code du travail. Une simple recherche sur le réseau LinkedIn permet de mesurer l'ampleur du phénomène.

LA PLACE DE L'INTELLIGENCE ECONOMIQUE

Nous avons vu que l'intelligence économique fait partie des 12 métiers identifiés dans l'étude précédente mais la réalité est un peu plus compliquée que cela. En effet, la cartographie des métiers[22] de l'intelligence économique dans l'entreprise (cf. figure ci-dessous) est beaucoup plus détaillée et montre bien la diversité des métiers qui compose l'IE et la complexité de la coordination de cette fonction au sein de l'entreprise.

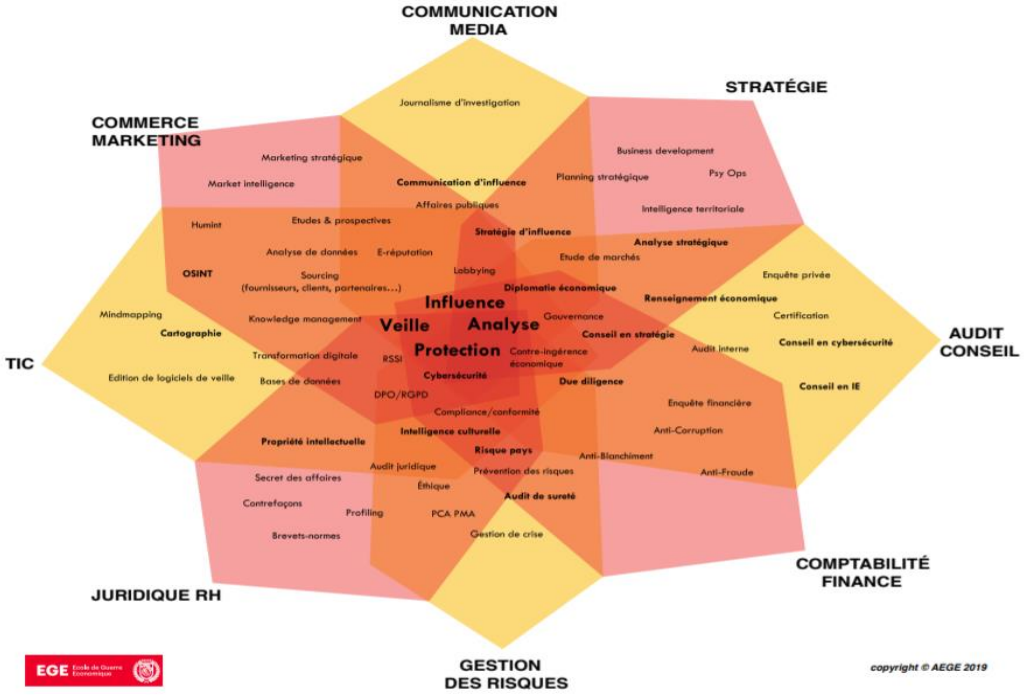


Figure 5 : Cartographie des métiers de l'IE par l'EGE/AEGE, mai 2019.

[22] Cartographie des métiers de l'IE : https://www.ege.fr/download/metiersIE_AEGE2019.pdf

L'IE doit être présente partout dans l'entreprise en étant confiée :

- A des responsables spécialisés dans le métier en question.
- A des employés qui ont d'autres responsabilités mais qui font un métier de l'IE dans leurs tâches/missions (parfois sans le savoir).
- A des prestataires externes (comme la veille ou l'influence).

On perçoit mieux la complexité de la tâche en termes de ressources humaines mais également en termes d'organisation et de coordination. C'est pourquoi les TPE/PME auront des difficultés à être efficientes dans ce domaine par manque de moyens ou parfois par ignorance des enjeux.

En France, il est régulièrement évoqué le retard des entreprises dans le domaine de l'IE (par rapport aux anglo-saxons) et notamment le manque d'accompagnement (ou de *leadership*) de l'État. Bien que des dispositifs nationaux [23] et locaux [24] existent pour accompagner et sensibiliser les entreprises, le fait d'en avoir modifié régulièrement les structures au cours des 20 dernières années (et notamment le rattachement aux services du 1er ministre ou à celui du ministre de l'Économie et des Finances) nuit au bon déroulé de leurs missions. Cela montre également que les enjeux de l'intelligence économique ne sont pas encore une priorité pour l'exécutif français et en tout cas loin de ce qu'il peut se faire aux États-Unis (cf. partie sur le *Homeland Security*).

Lors d'une déclaration en juin 2019 [25], Thomas Courbe, qui assure les fonctions de commissaire à l'information stratégique et à la sécurité économique (CISSE), semblait plus optimiste sur l'organisation de l'IE en France et sa prise en compte au plus haut sommet de l'État. Il insistait sur le fait que l'État devait collaborer davantage avec le privé dans ce domaine mais que les réponses se situaient souvent au niveau européen face au défi du patriotisme économique agressif des États-Unis ou de la Chine, représentait par les menaces pour nos entreprises que sont l'extraterritorialité du droit ou celui des investissements étrangers.

Pour le représentant du SYNFIE[26], Alexandre Medvedowski, les entreprises et en particulier les PME ne sont pas suffisamment armées en termes d'IE pour faire face à ces nouveaux risques que représentent ces nouvelles régulations (éthique des affaires, loi SAPIN 2, RGPD, …). En ce qui concerne les « agressions économiques étrangères » sur nos entreprises, il estime que l'État est encore trop naïf ou pas assez alerté de la situation. Il prône un changement de paradigme sur ce sujet entre l'État et les entreprises pour faire face aux menaces.

Sans aller plus loin dans l'analyse on peut supposer que le niveau des entreprises françaises (et notamment les PME) en termes d'organisation de l'intelligence économique est encore loin d'être à la hauteur des enjeux et des risques qui pèsent sur elles.

Peut-on penser que seuls les très grands groupes ont les moyens humains et financiers d'armer correctement les directions sûreté-sécurité des entreprises et notamment l'intelligence économique ? C'est ce que nous allons voir avec une autre étude récente du cabinet PricewaterhouseCoopers (PwC).

[23] Service de l'Information Stratégique et de la Sécurité Économique (SISSE).
[24] Au niveau des régions, des départements/préfectures et des Chambres de Commerce et d'Industrie.
[25] Lors d'une conférence organisée par le SYNFIE et l'EGE
[26] SYNFIE : Syndicat Français de l'Intelligence Économique

LE CAS DES GRANDES MULTINATIONALES

PwC est un réseau d'entreprises spécialisées dans des missions d'audit, d'expertise comptable et de conseil à destination des entreprises. Il fait partie des quatre grands cabinets d'audit et de conseil (Big Four) avec Deloitte, Ernst & Young et KPMG. (Voir chapitre sur les dépendances).

PwC France a conduit en 2018 une étude sur l'organisation et l'évolution de la fonction sûreté de certaines de ses entreprises clientes. Les similitudes avec l'étude du CDSE (notamment l'agenda) ne sont pas étrangères au fait que le responsable de l'étude chez PwC était l'ancien directeur général du CDSE.

Néanmoins, le périmètre est différent car les entreprises sondées ont déjà une certaine maturité dans le domaine sûreté-sécurité avec un profil suivant :

- 23 multinationales dont 20 qui ont de plus 20 milliards de dollars de chiffre d'affaires en 2017 et sont présentes dans plus de 60 pays.
- 10 nationalités représentées (11 européennes dont quatre françaises, quatre nord-américaines, trois asiatiques et une russe) dans des secteurs d'activités variés (banques, pharmaceutiques, luxe, aéronautique et défense, assurances, ingénierie …).
- Des effectifs importants (plus de 30 personnes) dédiés à la sûreté-sécurité au niveau Groupe (gouvernance et pilotage).

Nous allons présenter ici quelques résultats qui nous aiderons mieux appréhender le concept de sécurité globale appliqué aux grandes entreprises mondialisées.

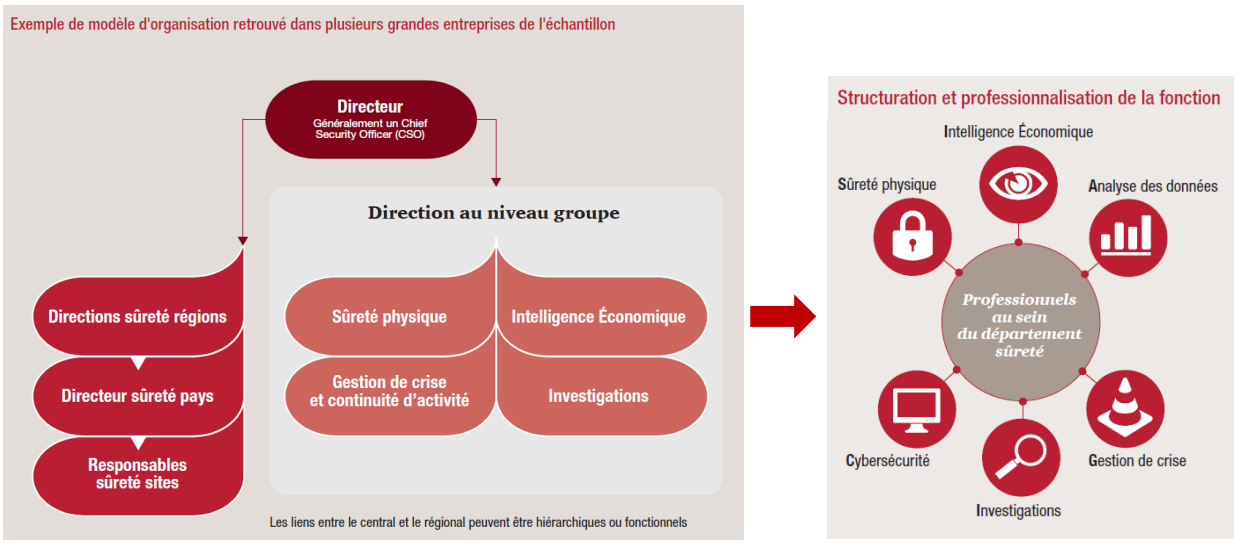


Figure 5 : Étude 2018 PwC « Transformation de la fonction sûreté ».

Les pratiques des entreprises concernant les DSS et qui sont misent en avant au travers de ce schéma (Figure 6) sont les suivantes :

- Centralisation des fonctions de gouvernance et de pilotage au sein d'une DSS au niveau Groupe (*corporate*).

- Structuration des fonctions sûreté entre le niveau Groupe – *corporate* et les filiales et/ou les zones géographiques.
- Professionnalisation de la fonction avec des métiers et filières d'expertises.
- Légitimation de la fonction : le responsable de la DSS est majoritairement rattaché à un membre du COMEX.

C'est cohérent avec l'étude du CDSE en tenant compte de la taille des entreprises (multinationales uniquement dans le cas de PwC) et donc du niveau beaucoup plus élevé de maturité des fonctions sûreté-sécurité.

Concernant la sécurité des systèmes d'information quelques constats sont à noter :

- Seuls 17% des RSSI sont directement rattachés au responsable de la DSS, contre 50% au DSI, le reste étant soit un mixte soit une autre fonction (audit, risque, innovation, digital).
- Mais 50% des entreprises confient des problématiques cyber également à la DSS et notamment la gestion de crise liée aux incidents de sécurité du système d'information.

Enseignement 3 :

Même si le décloisonnement entre les fonctions cyber et sûreté-sécurité est amorcé dans les grandes entreprises, il reste encore de nombreux domaines où la coopération peut être améliorée entre les fonctions, notamment la communication, l'échange d'information ou la sensibilisation des collaborateurs aux cybercrimes.

Le rôle de l'intelligence économique :

80% des entreprises interrogées possèdent des services d'intelligence économique dédiés, surtout dans les secteurs de la finance et de l'industrie. Celles qui n'ont pas de service interne externalisent des prestations d'IE.

Les équipes d'intelligence économique interagissent avec les DSS en effectuant :

- Des « due diligence » de tierces parties, notamment lors de décisions stratégiques (fusion/acquisition, choix d'un partenaire commercial, …).
- De la veille sur plusieurs secteurs : les marchés, la concurrence, les règlementations, la géopolitique, …
- De l'identification de vulnérabilités et analyse des risques sécuritaires.
- De la collecte de l'information dans le cadre d'investigation et soutien informationnel en gestion de crise.

Pour les grandes entreprises étudiées, ces cellules d'intelligence économique ont des moyens humains (jusqu'à 20 collaborateurs dédiés) et financiers conséquents et sont le plus souvent rattachées à la direction de la stratégie ou à la DSS.
Comme évoqué dans la partie précédente, les grands groupes semblent mieux armés pour couvrir l'ensemble du périmètre de l'intelligence économique.

Innovation de la part des DSS :

Pour couvrir ce besoin permanent de veille et d'analyse, les grands groupes internationaux des secteurs financiers et industriels ont mis en place des centres (internalisés) d'analyse de risques et de réaction (« *Security Operations Centers* ») qui assurent le monitoring de situations opérationnelles 24h/24, à l'image de ce qui est développé dans le domaine de la cybersécurité (mais le plus souvent externalisé).
Les missions principales de ces SOC sont :

- Recueillir les rapports d'étonnement des collaborateurs et favoriser l'échanges d'information au sein des entités (groupe, filiales, régions) de la DSS.
- Collecter, analyser et traiter les informations relatives aux menaces et aux risques de sûreté-sécurité et alimenter les bases de données.
- Collecter l'information dans le cadre d'investigation et assurer le soutien informationnel en cas gestion de crise, en interne et avec les autorités.

A noter que pour deux entreprises du secteur bancaire (qui comportent plus de cent collaborateurs à la DSS), et notamment *Bank of America* (plus de 300 collaborateurs à la DSS), ont également mis en place une « *fusion cell* » au sein de la DSS. Cette cellule composée principalement de spécialistes de la donnée (« *data scientist* » et « *data analyst* »), a pour but de tirer parti des nouvelles technologies (*big data*, intelligence artificielle, *machine learning*…) qui viennent en complément du SOC décrit plus haut :

- Agréger des données variées avec des outils spécialisés et les transformer en information utile pour les diffuser aux bons acteurs.
- Apporter des éléments d'analyse facilitant la prise de décision et en améliorant la capacité d'anticipation.
- Traiter l'information afin d'offrir une visualisation concrète (indicateurs de performance, tableaux de bord, …).

L'étude insiste aussi sur les moyens désormais alloués pour développer une culture sûreté-sécurité au sein de l'entreprise. Tous les moyens modernes (outils numériques, simulation, « *boot camp* », « *Serious Game* ») sont mis en place pour sensibiliser les collaborateurs aux menaces qui pèsent sur l'entreprise, et diminuer les comportements individuels à risque, notamment en cybersécurité et confidentialité.

UN EXEMPLE D'ORGANISATION EN LIGNES DE DEFENSE

PwC en tant que cabinet de conseil, profite de cette étude auprès de ses clients pour mettre en avant une organisation de la sûreté-sécurité présentée comme optimale. En effet, nous avons vu au travers de l'étude que plusieurs modèles d'organisations sont possibles pour les DSS. Tous les experts ou spécialistes ne sont pas rattachés directement à cette direction, avec un *reporting* direct au responsable. C'est souvent le cas pour les RSSI, les responsables

risques assurances, l'intelligence économique et notamment certaines veilles, sans compter la due diligence.

Comme la plupart des grandes directions des entreprises qui ont des enjeux stratégiques, la DSS se doit d'être contrôler voire évaluer et si possible de manière indépendante. PwC remarque que quelques entreprises étudiées mettent en place un système de ligne de défense. Néanmoins les entreprises n'ont pas fourni en détail cette organisation.
PwC se propose de décrire un modèle simplifié d'organisation en ligne de défense :

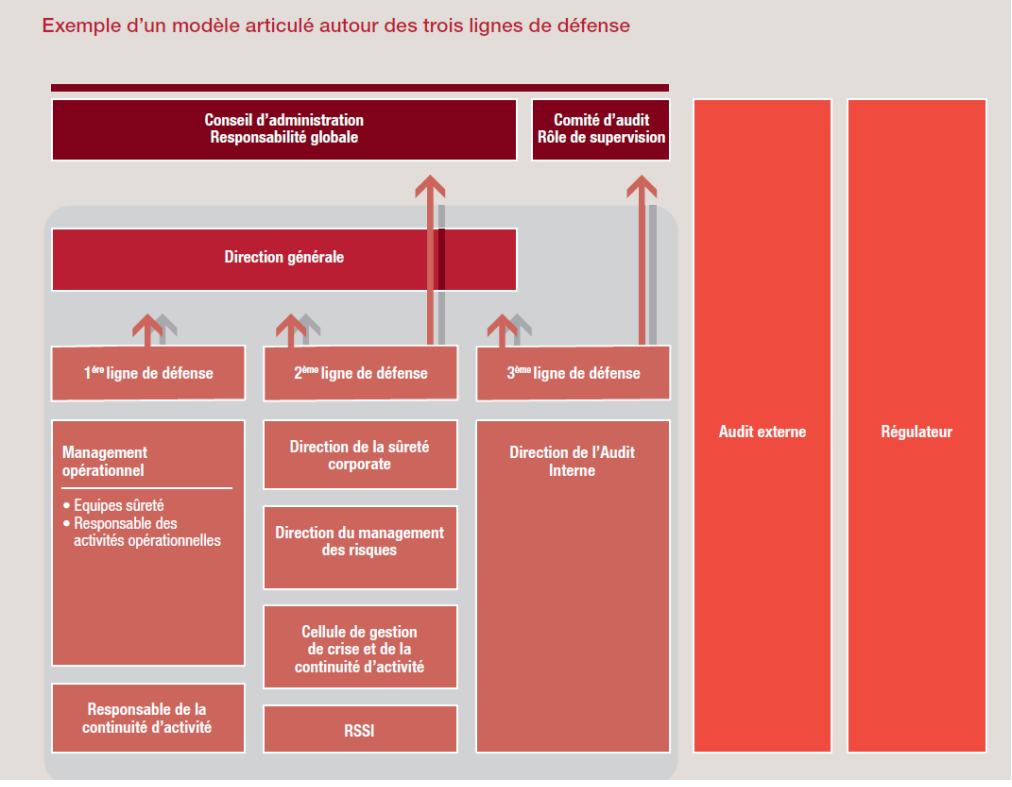


Figure 6 : Étude PwC 2018 « La transformation de la fonction sûreté »

La protection de l'entreprise ne s'articule plus autour de la DSS mais bien autour d'un système avec 3 lignes de défense/protection :

Ligne 1 : Elle regroupe la partie opérationnelle des activités de protection de l'entreprise, dans tous les domaines.

Ligne 2 : Centrée sur la gouvernance, elle regroupe les directions qui prennent part à la protection de l'entreprise (DSS, RSSI, management des risques, gestion de crise, juridique, …)

Ligne 3 : Elle est dédiée au contrôle de la DSS via l'audit interne de l'entreprise de façon indépendante. Le tout est complété par des audits externes qui sont parfois obligatoires (pour les professions réglementées comme la banque ou l'assurance) et effectués par des cabinets d'audit (PwC…) et des régulateurs (quand ils existent).

Selon l'auteur du rapport, moins de la moitié des entreprises interrogées mettent en œuvre des moyens de la troisième ligne, sans en détailler l'organistaion.

Enseignement 5 :

Cet exemple d'organisation en ligne de défense est pertinent pour couvrir l'ensemble du périmètre mais elle ne précise pas qui est à la tête de chaque ligne et qui coordonne toutes ces lignes. Si le pilotage de système de défense est confié au directeur sûreté-sécurité, ce dernier doit posséder une solide expérience de la protection de l'entreprise ainsi que des compétences dans des domaines très variés.

On peut également se poser la question des ressources humaines nécessaires, notamment à l'audit interne. En effet, il faut que cette direction possède des auditeurs ayant des connaissances dans tous les domaines de la sécurité-sûreté de l'entreprise, ce qui est rarement le cas. Une solution consiste à externaliser ces audits à des cabinets privés (comme PwC). Au-delà du coût, se pose alors la question de la confidentialité des données et des informations que ces cabinets d'audit (la plupart du temps anglo-saxons) récupèrent dans les entreprises…

Conclusion sur ces études :

En plus des moyens humains et financiers conséquents à mettre en place pour la protection des entreprises, leur organisation est un enjeu colossal qui ne semble pas encore mature, en particulier pour les PME. Si le décloisonnement entre certaines fonctions est amorcé (la sûreté, le cyber ou encore l'IE), nous n'avons pas trouvé d'entreprise qui dispose d'un véritable « comité de sécurité » avec à sa tête un leader dont le positionnement et les responsabilités sont supérieurs à des « simples » fonctions de directeur de la sûreté-sécurité.
Pour évaluer le niveau de protection des entreprises, une autre approche consiste à étudier leur gestion des risques et leur capacité à réduire leur niveau d'exposition face à ces risques qui s'accélèrent de plus en plus.

GESTION DU RISQUE ET TRANSFERTS ASSURANCIELS

DEFINITION

La gestion des risques ou *risk management* fait référence à la pratique consistant à identifier à l'avance les risques potentiels, à les analyser et à prendre des mesures de précaution pour en réduire ou en limiter l'impact. Une des toutes premières notions à définir sera celle de la criticité d'un risque, qui résulte en soit de la combinaison de l'impact (ou effet ou gravité) et de la probabilité d'un risque. Ainsi nous sommes en mesure de classer les risques par indice de criticité.

Lorsque l'on décide de parler de gestion de risque, il faut tout d'abord commencer par savoir de quel secteur nous parlons, car ils n'ont évidemment pas la même maturité selon les exigences de conformité.

La primo analyse de façon générale serait distribuée selon ces 4 problématiques :

1. Analyse sectorielle et statut de l'entreprise ? (OIV, OSE, PP, ...)
2. Niveau d'attractivité du secteur en question ?
3. Les exigences intrinsèques ? (normes, conformité, cadres légale, …)
4. Le niveau de maturité de l'entreprise ?

Par exemple : *les normes ISO27005, ISO31000, EBIOS/ EBIOS Risk Manager, … sont des outils nous permettant de réaliser des analyses de risques.*

D'une analyse de risque type EBIOS Risk Manager, découlera ensuite une partie de la définition d'une PSSI (Politique de Sécurité des Systèmes d'Informations) par exemple.

LE TRAITEMENT DU RISQUE

Afin d'introduire la suite des explications, il est important de comprendre que le responsable de la gestion des risques au sein d'une entreprise doit adapter la stratégie de l'entreprise avec la gestion des risques. Au sein des grands groupes, ce sont généralement des départements « *Risk Management* », souvent proches de la « DAF » mais pour les plus petites entreprises, il est souvent coûteux de faire appel à des conseils et cette fonction dite « support » ne pourrait pas justifier une création de poste en interne. Il apparait donc que le management des risques en entreprises est une question de moyens financier et de « sensibilité » également du secteur d'activité.

Si nous prenons en exemple le cas d'une PME française d'environ une quinzaine de salariés. Leur cœur de métier est la gestion des données en transit entre les pacemakers et les bases de données de traitements des hôpitaux. Et bien dans ce contexte particulier ou la vie du patient dépend du bon traitement peut faire appel a des cabinets d'audits plusieurs fois par ans pour divers contrôles. Ces échanges donc multicanaux canaux pacemakers – PME – hôpitaux sont extrêmement sensibles. Le traitement informatisé des données médicales est soumis par exemple à des exigences relatives à la règlementation de l'hébergement des

données de santé. Ainsi, cette société, si modeste qu'elle soit se voit dans l'obligation de réitérer des analyses de risques plusieurs fois par ans et sur différents périmètres bien spécifiques de son activité.

Sans garanties de conformités, nulle entreprise ne peut exercer une activité dans un secteur spécifique tel que celui cité ci-dessus et, la gestion du risque est une des clefs de celles-ci.

Nous allons maintenant procéder à la description d'un processus de gestion du risque dans son ensemble dans le point suivant :

1. Identification du Risque :

Input	Identification du risque	Output
Résultats des précédents audits	Identification des actifs (primordiaux et de support) • Lise des actifs primordiaux (processus et informations) • Liste de actifs support (Locaux, organisation et personnes, systèmes d'information..)	Inventaires des actifs
Critères de valorisation des actifs	Valorisation des actifs (C, I et D)	Valorisation des actifs
Sources de menaces	Identification des mesures existantes	Liste des mesures par famille d'actifs
Bases de scénarios EBIOS	Identification des menaces et des vulnérabilités	Liste des menaces et des vulnérabilités par famille d'actifs
Workshops avec les responsables métiers	Identification des scénarios de risques	Scénarios de risques identifiés pour chaque famille d'actifs

2. Analyse du Risque & Évaluation du Risque :

Input	Analyse du Risque	Output
Scénarios de menaces	Identifier des conséquences (impact) des scénarios de risques	Identifier pour chaque scénario de risque un : • Niveau d'impact et de vraisemblance • Niveau de risque
Mesures existantes	Identification de la probabilité (vraisemblance) des scénarios de risques	
Echelles de calcul du risque Workshops avec les responsables métiers	Calcul du niveau de risque	
Input	**Evaluation du Risque**	**Output**
Critères de gestion et d'acceptation du risque	Classification et pondération des niveaux de risque	Liste des risques à traiter
Workshops avec les responsables métiers	Identification des risques à traiter	

3. Processus de gestion des risques en 7 points clefs :

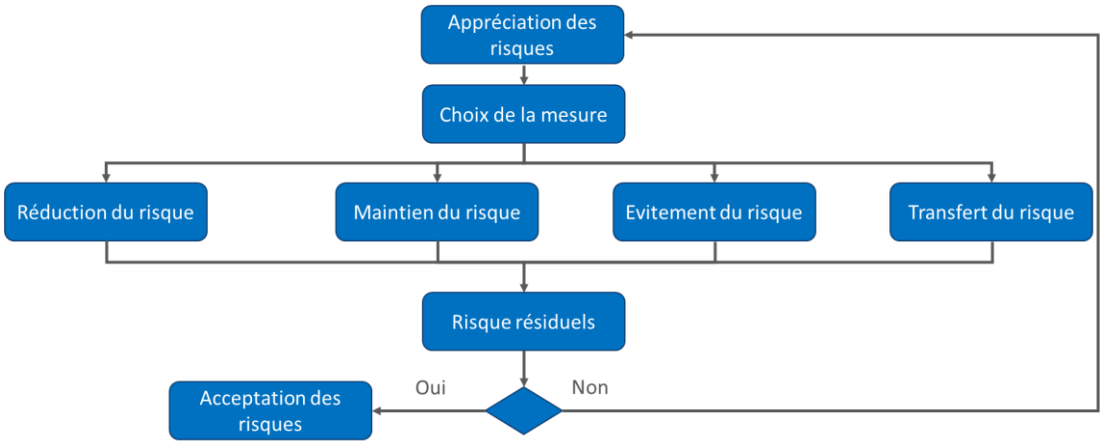
- **Établissement du contexte** : La compréhension de l'organisme est essentielle avant de débuter un projet d'appréciation du risque. L'objectif principal de cette première activité est d'identifier globalement le système qui sera traité et de le situer dans son environnement interne et externe.
- **Appréciation du risque :** Ensemble du processus d'identification des risques, d'analyse du risque et d'évaluation du risque.
- **Identification du risque** : Processus utilisé pour trouver, lister et caractériser les éléments à risque.
- **Estimation du risque** : Processus utilisé pour affecter des valeurs à la probabilité et aux conséquences d'un risque.
- **Évaluation du risque** : Processus de comparaison des résultats de l'analyse du risque avec les critères de risque afin de déterminer si le risque et/ou son importance sont acceptables ou tolérables.
- **Traitement du risque :** Processus destiné à modifier un risque : Réduction du risque – Maintien du risque – Évitement du risque – Transfert du risque.
- **Acceptation du risque :** prendre la décision d'accepter les risques.

4. Cartographie des risques :

Dans le cadre de démarches de gestion du risque, la cartographie des risques consiste à recenser les risques et à les synthétiser sur un document dans lequel ils seront placés en tenant compte de l'impact en cas de survenance du risque et de la fréquence de réalisation du risque.

5. Traitement du risque cyber :

Le traitement du risque implique le choix et la mise en œuvre de plusieurs mesures de modification des risques.



6. Les options de traitement du risque cyber :

- Réduction du risque : Choisir les mesures de sécurité à mettre en place pour réduire le risque afin que le risque résiduel puisse être accepté.
- Maintien du risque : Décision d'acceptation du niveau du risque (exemple : lorsque les couts de mise en œuvre des mesures de sécurité sont supérieur à la perte potentielle par la réalisation du risque).
- Évitement du risque : Abandonner l'activité (couts de mise en œuvre des mesures de sécurité > les bénéfices attendus).
- Transfert du risque : Partager les risques avec des parties externes (Assurance Cyber / Externalisation).

7. Plan de traitement des risques :

Après le choix des mesures de sécurité à mettre en place pour réduire le risque, il convient d'identifier et de planifier les activités de traitement des risques. Pour cela, il faudra :

- Classer les mesures de sécurité par ordre de priorité.
- Allouer les ressources nécessaires.

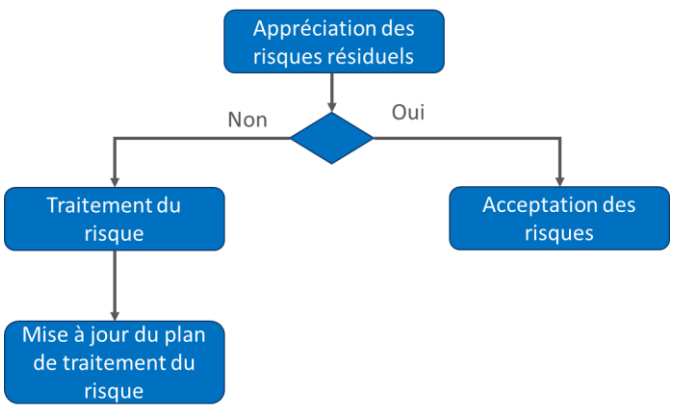
Exemple :

Risque	Mesures de sécurité	Option de traitement	Niveau de risque	Priorité	Responsable
Fuite de données suite à un accès non autorisé depuis le réseau interne	Vérifier régulièrement les droits d'accès des utilisateurs et la robustesse des mots de passe utilisés et supprimer les comptes génériques	Réduction du risque	Haut	Haute	N/A

8. Évaluation des risques résiduels :

Risque résiduel : le risque qui subsiste après la mise en place des mesures de sécurité pour atténuer le risque inhérent.

Risque inhérent : le risque sans prise en compte des mesures de sécurité.



LA STRATEGIE DE GESTION DU RISQUE

La bonne question à se poser est la suivante : Comment faire pour couvrir un risque ?

Une première réponse est déjà d'avoir une conscience spécifique de ce risque et d'être en mesure d'identifier ses *assets* critiques. Une « interruption métier » dans le secteur de l'Industrie a par exemple un impact considérable sur le *business.*

Des analyses de risque techniques et standards ne permettent pas d'apprécier correctement ce risque. Il doit s'opérer une véritable synergie entre les organisations (souvent en silos) des entreprises afin que d'un effort collaboratif puisse être élaboré des scénarii catastrophes afin d'en déterminer l'impact réel.

La seconde réponse serait également de comprendre le point de vu assurantiel. Ainsi ce type de problématique se traitera en lien direct avec les sociétés d'assurance ou de réassurance. Car les calculs d'impacts sur base de scénarios catastrophe permettent de définir des PML (*Possible Maximum Loss),* nous parlons alors de calculs d'impacts majorants. Si nous souhaitions montrer l'équivalent d'un scénario catastrophe cyber type « Not Petya », alors nous pourrions prendre en exemple le cas de Fukushima. Accident où la conjonction des risques : séisme et tsunami, frappant des installations nucléaires. Cette convergence a très faible probabilité s'est produite, il est donc nécessaire dans la gestion des risques d'élaborer des scénarios sur un large spectre d'impacts.

La production de matrices de risques comprenant le *scoring* menaces, le renseignement sur les menaces, des travaux de veille et d'analyse permettent une appréciation de la menace au plus proche de la réalité. Ainsi des cellules dédiées au sein des entreprises sont constituées aujourd'hui.

Évolution récente notable :

Dans la gestion de risques d'une entreprise, il faut pouvoir également être en capacité d'apprécier le risque chez ses sous-traitants. Les cabinets d'audits et de conseils ont de plus en plus de missions chez les fournisseurs et divers acteurs en lien d'un même secteur, et ce, pour plusieurs raisons :

- soit pour des exigences de conformité au niveau légal,
- soit à la demande des entreprises-clientes,
- ou bien même et de plus en plus à la demande des compagnies d'assurances.

En Conclusion nous viendrons citer une étude issue de la revue des Sciences de Gestion, qui a tiré des enseignements du Committee of Sponsoring Organizations of the Treadway Commission (COSO II), « The enterprise Risk Management- Integrated Framework » et de l'écrit « Le management des risques de l'entreprise » (IFACI et PriceWaterhouse Coopers).

« Les temps ont changé et les faits ont montré que la vieille approche des silos hiérarchiques (fabrication, études, ventes, marketing, administration…) en management des risques n'était plus suffisante. Ainsi, une nouvelle approche du management des risques a été développée. Elle s'appelle le Management des risques d'entreprise qui prône une approche intégrée et rigoureuse des risques en évaluant et en localisant les risques dans toutes les zones qui pourraient avoir un impact sur la stratégie de l'organisation et ses différents objectifs. Bien qu'il y ait de nombreux avantages à retirer du Management des risques d'entreprise, le principal avantage demeure sa capacité à éviter de grosses pertes. Si le risque peut être pris en compte et bien géré, des pertes lourdes peuvent être évitées. »

LES ENJEUX DE LA CYBERSECURITE POUR L'ENTREPRISE

« La cybercriminalité est un groupe d'infractions pénales qui peuvent être commises via Internet. Il s'agit de la définition des infractions commises sur la toile. L'explosion du numérique et la simplification de l'accès à l'informatique ont donné naissance à une toute nouvelle forme de délinquance. »

92% des entreprises françaises ont subi une ou plusieurs cyberattaques en 2018. Ce chiffre est impressionnant d'autant que les cyberattaques ne sont pas toujours détectées.[27]

- 22 % des entreprises ne détectent aucune cyberattaque durant l'année.
- 20 % ont détecté une seule cyberattaque.
- 31 % en ont détecté 2 à 5.
- 15 % en ont détecté plus de 5.

En 2018, le risque cyber était classé parmi les plus grandes inquiétudes des dirigeants comme des États. La cybersécurité a très vite été identifiée comme faisant partie du cercle de la sécurité globale.[28]

Avec l'augmentation de la présence des petites et grandes entreprises dans le cyberespace, les risques en matière de cybercriminalité n'ont jamais été aussi élevés. Les grands groupes comme les PME sont dans le collimateur des cybercriminels.

La cybersécurité est aujourd'hui un enjeu stratégique à ne pas négliger si l'on veut que l'entreprise soit efficiente dans la durée. Et il sera toujours plus coûteux d'intervenir après un incident que de manière préventive en anticipant les risques. Il vaut mieux prévenir que guérir même en sécurité. En effet, les répercussions suite à une mauvaise évaluation des risques cyber sont nombreuses, imprévisibles et il est difficile de les chiffrer en amont.

Le coût global de la cybercriminalité atteindra 6 000 milliards de dollars d'ici 2021.[29]

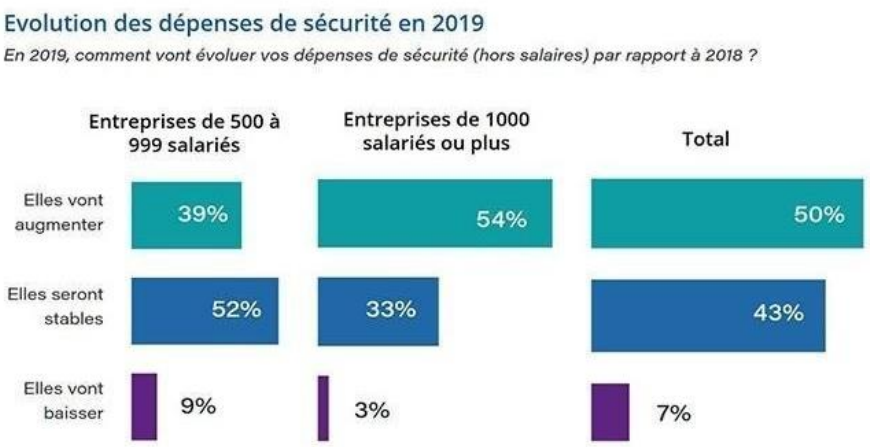


Figure 7 : Evolution des dépenses de sécurité en 2019

[27] F-Secure, Le trafic des cyberattaques, 5 Mars 2019
[28] Baromètre cybersécurité 2019 Sylob, Usine Nouvelle et Hub One, 21 Février 2019
[29] Quelles sont les différents types de cybercriminalité, Panda Security, 23 Janvier 2019

Toutefois, résumer la cybersécurité à un panel de solutions techniques à mettre en place est une vision trop simpliste de celle-ci. La cybersécurité est un ensemble d'outils, de techniques, de connaissances et de bonnes pratiques qui permet de réduire au maximum les risques. Les entreprises doivent se sentir concernées par leur propre cybersécurité et c'est en formant un bloc solide, cohérent et conscient qu'elles pourront résister au mieux aux attaques et faire monter le niveau de sécurité globale.

Le *ransomware* est cette année encore la cyber-attaque la plus fréquente, loin devant les attaques virales générales et la fraude externe ou les vols d'information.

Dans le même temps, deux types d'attaques sont moins fréquentes qu'en 2017 : les attaques par déni de service (DDoS) et la défiguration de site web. Le social engineering et les vulnérabilités résiduelles permanentes touchent une entreprise sur deux et viennent compléter le tableau des cyber-risques auxquels les entreprises sont les plus exposées.

LA GENESE DE LA CYBERCRIMINALITE

Le lien malveillant avec le piratage informatique a été documenté pour la première fois dans les années 1970, lorsque les premiers téléphones informatiques sont devenus une cible. Les experts en technologie connus sous le nom de « *phreakers* » ont trouvé un moyen de payer les appels longue distance grâce à une série de codes.[30] Ils ont été les premiers pirates, apprenant à exploiter le système en modifiant le matériel et les logiciels pour voler du temps de téléphone longue distance. Cela a fait prendre conscience aux gens que les systèmes informatiques étaient vulnérables aux activités criminelles et que plus les systèmes étaient complexes, plus ils étaient sensibles à la cybercriminalité.

En 1990, un grand projet nommé « *Operation Sundevil* » a été exposé. Les agents du FBI ont confisqué 42 ordinateurs et plus de 20 000 disquettes utilisées par des criminels à des fins d'utilisation illégale de cartes de crédit et de services téléphoniques.

Cette opération a impliqué plus de 100 agents du FBI et il a fallu deux ans pour retrouver la trace de seulement quelques suspects. Cependant, cela a été perçu comme un bel effort de relations publiques, car c'était un moyen de montrer aux pirates informatiques qu'ils seraient surveillés et poursuivis en justice.

L'Electronic Frontier Foundation a été créée pour répondre aux menaces qui pèsent sur les libertés publiques lorsque les forces de l'ordre commettent une erreur ou participent à des activités inutiles pour enquêter sur un cybercrime. Leur mission était de protéger et de défendre les consommateurs contre des poursuites illégales. Bien qu'utile, cela a également ouvert la porte aux échappatoires des hackers et à la navigation anonyme où de nombreux criminels pratiquent leurs services illégaux.

Le crime et la cybercriminalité sont devenus un problème de plus en plus important dans notre société, même avec le système de justice pénale en place. Dans l'espace web public comme dans le Dark Web, les cybercriminels sont hautement qualifiés et difficiles à trouver.

[30] Une analyse économique du piratage informatique, Revue de Sciences humaines, Peter T. Leeson, 1er Janvier 2017

La cybercriminalité est le troisième plus grand fléau économique dans le monde, derrière la corruption dans le secteur public et le trafic de stupéfiants.

En France, en 2008, pour renforcer la cohérence et la capacité propre des moyens de l'État en matière de sécurité des systèmes d'information, à l'instar des principaux partenaires de la France, le Livre blanc sur la défense et la sécurité nationale prévoit la création d'une agence nationale de la sécurité des systèmes d'information (ANSSI).

Cette agence relève du Premier ministre et est rattachée au secrétaire général de la défense nationale. Le 8 juillet 2009 l'ANSSI voit le jour à la suite d'une mission de préfiguration mise en place dès le 1er janvier 2009.

Cette agence se substitue à l'actuelle direction centrale de la sécurité des systèmes d'information (DCSSI) tout en en renforçant les compétences, les effectifs et les moyens.

L'agence nationale de la sécurité des systèmes d'information a notamment pour mission :

- de détecter et réagir au plus tôt en cas d'attaque informatique, grâce à la création d'un centre opérationnel renforcé de cyberdéfense, actif 24 heures sur 24, chargé de la surveillance permanente des réseaux les plus sensibles de l'administration et de la mise en œuvre de mécanismes de défense adaptés.
- de prévenir la menace : l'agence contribuera au développement d'une offre de produits et de services de confiance pour les administrations et les acteurs économiques.
- de jouer un rôle permanent de conseil et de soutien aux administrations et aux opérateurs d'importance vitale.
- d'informer régulièrement les entreprises et le grand public sur les menaces et les moyens de s'en protéger, en développant une politique de communication et de sensibilisation active.[31]

LES VECTEURS DE VULNERABILITES DE L'ENTREPRISE

LES TYPOLOGIES DE MENACES

Il existe, aujourd'hui, plusieurs types de cybercrimes.

Les attaques DDoS

Celles-ci servent à rendre un service en ligne indisponible et à détruire le réseau en submergeant le site de trafic provenant de diverses sources. Les grands réseaux de périphériques infectés, appelés botnets, sont créés en déposant des logiciels malveillants sur les ordinateurs des utilisateurs. Le pirate informatique pirate ensuite le système lorsque le réseau est en panne.

[31] Agence Nationale de la Sécurité des Systèmes d'information

Les botnets

Les botnets sont des réseaux d'ordinateurs compromis contrôlés de manière externe par des pirates informatiques à distance. Les pirates envoient ensuite des spams ou attaquent d'autres ordinateurs via ces botnets. Ils peuvent également être utilisés pour agir en tant que virus et effectuer des tâches malveillantes.

Le vol d'identité

Ce cybercrime se produit lorsqu'un criminel obtient l'accès aux informations personnelles d'un utilisateur pour lui voler de l'argent, accéder à ses informations confidentielles ou participer à une fraude fiscale ou une fraude à l'assurance maladie. Ils peuvent aussi ouvrir un compte téléphonique ou internet à votre nom, utiliser votre nom pour planifier une activité criminelle et réclamer les aides que vous donne le gouvernement. Pour ce faire, ils piratent les mots de passe de l'utilisateur et récupèrent des informations personnelles sur les réseaux sociaux ou en envoyant des emails de phishing.

L'ingénierie sociale (Social Engeenering)

L'ingénierie sociale fait référence à des pratiques de manipulation psychologique à des fins d'escroquerie. Les criminels vous contactent directement, habituellement par téléphone ou par email. Ils veulent gagner votre confiance et se font passer pour l'agent d'un services clientèle afin que vous lui fournissiez les informations dont il a besoin. Il s'agit généralement d'un mot de passe, du nom de l'entreprise pour laquelle vous travaillez ou vos coordonnées bancaires. Les cybercriminels trouveront ce qu'ils peuvent à propos de vous sur internet puis tenteront de vous ajouter comme ami sur les réseaux sociaux. Une fois qu'ils ont accès à un compte, ils peuvent vendre vos informations ou sécuriser des comptes en votre nom.

Le phishing

Ce type d'attaques implique que des pirates informatiques envoient des pièces jointes ou des URL malveillantes à des utilisateurs pour accéder à leurs comptes ou à leur ordinateur. Les cybercriminels sont de plus en plus déterminés et nombre de ces emails ne sont pas signalés comme spam. Les utilisateurs sont piégés dans des emails affirmant qu'ils doivent changer leur mot de passe où mettre à jour leurs informations de facturation, donnant ainsi accès aux criminels.

LE FACTEUR HUMAIN

Les salariés ont besoin d'être sensibilisés au risques cyber. Les entreprises en sont de plus en plus conscientes. Les erreurs humaines font parties des principales erreurs relevées suite à une cyberattaque.

Pour se protéger au maximum, l'entreprise n'a pas d'autre choix que de passer irrémédiablement par la mobilisation de toutes ces parties prenantes. 97% des attaques utilisent le facteur humain pour arriver à leurs fins.

Il faut donc éduquer, sensibiliser les utilisateurs et les directions générales. Cela passe aussi par de la communication.

Chaque utilisateur a son rôle à jouer en matière de sécurité. Leur éveil, conscience et compréhension des risques est indispensable. Quels que soient les systèmes de protection mis en place, à un moment donné ce sera l'utilisateur qui, s'il n'a pas conscience des risques, cliquera sur un lien malveillant, ouvrira une pièce jointe compromise, ou divulguera une information sensible à la mauvaise personne sans penser mal faire.

LA PENURIE DE RESSOURCES HUMAINES

Le secteur de la cybersécurité cherche aujourd'hui, en France, plus de 5 000 personnes. Tous les ans, ce sont plusieurs milliers de nouveaux postes qui sont à pourvoir dans les entreprises, les administrations ou les collectivités locales. Et ces chiffres devraient encore augmenter.

Le conflit grandissant entre l'univers de la cybercriminalité et celui du monde de l'activité privée est une guerre à la fois technologique, mais aussi organisationnelle et culturelle.

L'étude "Cybersecurity Workforce" de (ISC)2, un organisme de formation et de certification aux métiers de la cybersécurité, avance que presque trois millions d'employés dédiés à la cybersécurité manqueraient dès aujourd'hui au niveau mondial.

De surcroît, il n'y aurait, au niveau mondial, que 10-15% de femmes parmi le personnel dédié à la cybersécurité. Cette absence des femmes est dangereuse désormais par rapport au manque de talents en cybersécurité. Dans un monde où la cybersécurité devrait être de plus en plus comprise comme une problématique collective, où tout le monde doit être capable de parler avec tout le monde, et comprendre a minima ce que fait le voisin.

LA GESTION DES DONNEES ET LE RGPD

Le RGPD ajoute un coût financier aux entreprises, mais aussi surtout une charge supplémentaire pour le RSSI, qui cumule parfois la fonction de DPO. D'autant plus que la plupart des entreprises n'ont pas terminé leurs chantiers de mise en conformité RGPD.

Le 25 mai 2018 est entré en vigueur le RGPD (Règlement Général sur la Protection des Données). Il concerne toutes les entreprises dès lors qu'elles manipulent des données personnelles, c'est-à-dire relatives aux personnes physiques identifiées ou identifiables, directement (par leur nom…) ou indirectement (par un numéro de téléphone, un numéro client…).

Ce règlement vise à renforcer les droits des utilisateurs (droits d'accès aux données, d'opposition, d'effacement, de portabilité…). Il entend, par ailleurs, responsabiliser les acteurs impliqués dans le traitement des données personnelles. À cette fin, il oblige les entreprises mais aussi leurs sous-traitants à prouver leur « accountability », c'est-à-dire à mettre en place des procédures internes destinées à démontrer le respect des règles.

Le RGPD prévoit aussi la réalisation d'une Analyse d'Impact relative à la Protection des Données (AIPD) si leur traitement est susceptible d'engendrer un risque élevé pour les droits

et les libertés des personnes concernées. Enfin, autre point notable : si vous constatez une violation de sécurité, vous devez en informer la CNIL et selon les cas, les usagers touchés. L'absence de conformité au RGPD vous expose à des sanctions pouvant atteindre 20 millions d'euros ou 4 % de votre chiffre d'affaires annuel mondial.

LES ENJEUX POUR L'ENTREPRISE

LE COUT FINANCIER

Les entreprises n'en sont plus à se poser la question de si elles vont être victimes d'une attaque cyber mais plutôt de savoir quand et comment elles le seront. La croissance des sources et modes d'attaques doit conduire les entreprises à s'organiser pour les affronter.

175 milliards de téraoctets : c'est le volume de données qui devrait être stocké en 2025 dans le monde entier.

Bonne nouvelle pour les hackers. Mais pour les entreprises, cibles potentielles, elle rappelle l'importance des questions de cybersécurité. Et les enjeux sont d'autant plus forts que la dépendance aux outils numériques continue de grandir parmi les professionnels, que le recours au Cloud se généralise et que les objets connectés se multiplient.

La gestion du risque et de l'attaque représente donc d'abord un enjeu financier direct puisqu'il va s'agir de sécuriser les données, d'informer les clients, de faire appel à des avocats et à des experts en relation publique.

À cela s'ajoute la perte de chiffre d'affaires susceptible d'être enregistrée en attendant le rétablissement complet du système.

Un rétablissement dont le délai est estimé en moyenne à 69 jours une fois la violation de données détectée. Au-delà des conséquences immédiates et pour une évaluation juste du coût des risques cyber, il faut aussi prendre en compte les impacts indirects (sur une durée plus ou moins longue selon l'ampleur de la crise), comme la perte de confiance de la part des clients et des partenaires, les sanctions financières appliquées en cas de défaut de sécurité, la divulgation d'informations portant atteinte à votre compétitivité… Au total, en moyenne, les entreprises françaises évaluent leurs pertes à 9,36 % de leur chiffre d'affaires en cas de violation de sécurité.

LA SOUVERAINETE NUMERIQUE

Une révolution numérique se met en place. Les nouvelles technologies ou technologies émergentes sont en passe de bouleverser le monde des entreprises.

Le Cloud, l'Internet 2.0 et les media sociaux, le Big Data, les objets connectés offrent de nouvelles opportunités « business » pour les entreprises que ce soit dans la création de nouveaux produits et services, ou dans le développement de la relation et négociation client.

En conséquence, le patrimoine digital se développe dans toutes les entreprises et devient à la fois un élément clé pour leur fonctionnement et un capital vital à protéger pour maintenir leur position concurrentielle vis-à-vis de l'ensemble de leurs compétiteurs, à échelle mondiale.

Cette révolution et cette recherche de souveraineté numérique a donc également des répercussions sur la sécurité des entreprises. Leur niveau d'exposition aux risques en général et aux risques cyber en particulier est depuis quelques années en perpétuelle augmentation et est devenu un sujet d'attention et de préoccupation pour les dirigeants des entreprises.

La mondialisation et la numérisation du monde des affaires et des échanges commerciaux ont fait apparaître de nouvelles sources et de nouveaux types de menaces.

Les entreprises hébergent une multitude d'informations qui attirent la convoitise, que ce soit de la part de compétiteurs dans un contexte de guerre économique. Ces mêmes entreprises évoluent au sein d'un écosystème de plus en plus interconnecté et ouvert, et offrent donc une exposition de plus en plus large aux intrusions et aux attaques qui peuvent être initiées depuis n'importe quelle partie du monde.

Il faut noter également que le nombre de cybercriminels est en très forte augmentation et que leurs pratiques se professionnalisent et deviennent de plus en plus sophistiquées. Les hackers d'autrefois (en recherche de notoriété liée à leurs « performances ») ont désormais laissé la place à des experts du cybercrime dont la principale motivation est de gagner de l'argent, ou recrutés par des États en quête d'information stratégique.

En conséquence, les entreprises doivent repenser leurs modèles de gestion des risques et de crise, pour intégrer la dimension numérique croissante dans les crises.

Cet écosystème n'est pas en phase avec la situation économique actuelle de la France et d'un point de vue global de l'Europe. Dans le monde de l'entreprise, à l'émergence de la puissance économique américaine, la France a accepté la notion de dépendance.[32]

Du côté des entreprises françaises, elles donnent malheureusement l'impression qu'il est déjà trop tard.

En France, il n'existe pas d'harmonie de pensée entre le monde politique, l'appareil d'État et le monde de l'entreprise.

Pour Christian Harbulot, Directeur de l'École de Guerre Économique, il existe trois types d'urgence :

- Il faut mettre le monde de l'entreprise devant ses responsabilités. Les entreprises refusent aujourd'hui de rentrer dans ce rapport de force. Il y a eu des tentatives mais toutes se sont avérées vaines. Les entreprises n'ont pas su travailler dans un objectif d'intérêt général.
- Le cadre européen : L'Europe est dépendante du monde américain. In fine, l'Europe aura sans doute une double dépendance – les États-Unis et la Chine.
- L'organisation du commerce des données dans le secteur privé. Dans le domaine des technologies bancaires, les États-Unis ont déjà beaucoup d'avance. La RGPD ne suffit pas pour régler cette problématique. Il faut lever la barre au niveau stratégique.

[32] Commission d'enquête sur la souveraineté numérique, 23 Mai 2019

La réelle problématique des entreprises françaises est que les actionnaires sont de moins en moins français et de ce fait elles tendent à suivre la législation des nationalités de ces actionnaires.

Les entreprises françaises ont les capacités pour rattraper leur retard en prenant l'exemple de ce qu'il s'est fait ailleurs. Il faut utiliser tous les moyens à disposition des États, des entreprises.

LES COUTS DE LA CYBERCRIMINALITE DANS LE MONDE

Le coût de la cybercriminalité varie selon les régions et le niveau de cybersécurité de chaque pays. Les États les plus riches subissent des pertes très élevées. Les pays les plus touchés par les cyberattaques sont les pays de taille intermédiaire.

- **Allemagne :** Le pays héberge l'économie Internet souterraine la plus sophistiquée de l'Union européenne.
- **Brésil : Il** représente la deuxième source majeure de cyberattaques et la troisième cible la plus touchée.
- **Émirats arabes unis :** Il s'agit du deuxième pays le plus ciblé et dont le coût de la cybercriminalité est estimé à 1,4 milliard de dollars par an.
- **Japon :** Jusqu'il y a peu protégé contre la cybercriminalité par la barrière linguistique et l'absence d'infrastructure pour le blanchiment d'argent, le Japon a connu une augmentation des attaques, surtout celles lancées contre les banques.
- **Royaume-Uni :** Les fraudes en ligne et la cybercriminalité représentent près de la moitié de l'ensemble des activités criminelles, avec plus de 5,5 millions de délits chaque année.

La cybercriminalité atteint un niveau record, coûtant chaque année des milliards de dollars aux entreprises et aux particuliers. Le plus effrayant, c'est que ce chiffre ne représente que les 5 dernières années sans espoir que cela se termine un jour. L'évolution de la technologie et l'accessibilité croissante des technologies intelligentes signifient qu'il existe de nombreux points d'accès aux domiciles des utilisateurs à exploiter. Tandis que les forces de l'ordre tentent de s'attaquer au problème croissant, le nombre de criminels continue de croître, profitant de l'anonymat d'Internet.

LA CYBER-RESILIENCE

DEFINITION

La cybersécurité devient un pan de la cyber-résilience

En 2019, les entreprises intelligentes ne considéreront plus la cybersécurité comme une fonction distincte du service informatique, mais comme un modèle à adopter pour toute l'entreprise.

Ce concept de cyber-résilience regroupe la sécurité de l'information, la continuité de l'activité et la résilience dans le but de former des systèmes sécurisés de par leur conception, et non

suite à une réflexion après coup. Les entreprises peuvent ainsi se concentrer sur leurs capacités à exploiter leurs activités en continu, malgré les cyberattaques ou les incidents.

Un programme de cyber-résilience robuste implique :

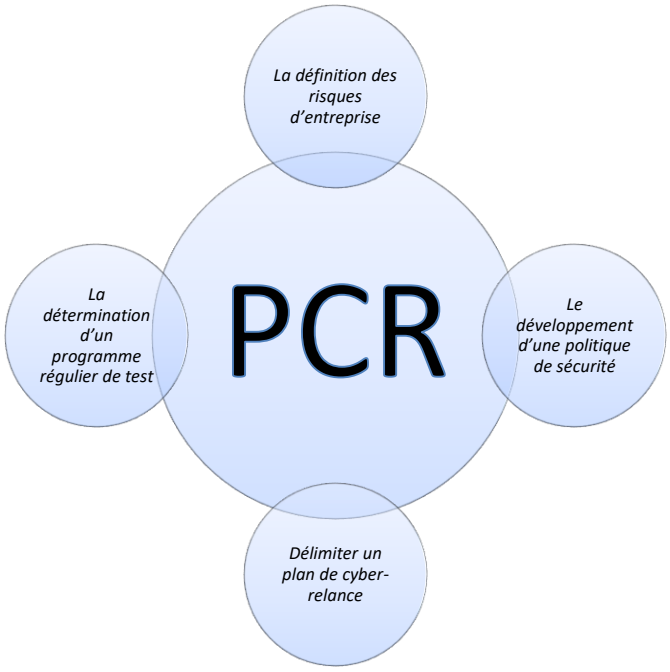


Figure 8 : Un programme de cyber-résilence robuste

La cybersécurité consiste à réduire les risques d'intrusion, d'attaques ou les effets de catastrophes naturelles ou causées par l'homme dans le cadre de l'utilisation des moyens informatiques et de communication, alors que la cyber-résilience est la capacité à se préparer et s'adapter à des conditions en perpétuelle évolution ainsi qu'à récupérer rapidement ses capacités suite à des attaques délibérées, des accidents, des catastrophes naturelles ou encore des incidents dans le cadre de l'utilisation de moyens informatiques et de communication.

La résilience est la capacité à préparer et à s'adapter à des conditions changeantes, de résister et de récupérer rapidement suite à des perturbations subies. La résilience comprend la capacité de résister et de se remettre d'attaques délibérées, d'accidents, ou de catastrophes naturelles ou encore d'incidents.

Le préfixe Cyber, pour sa part fait référence à toutes les techniques liées à la société du numérique et notamment à l'informatique et à l'internet.

Il résulte de ces deux définitions que le périmètre de cybersécurité couvre essentiellement la réduction des risques et la résolution des incidents de sécurité de l'information alors que la cyber-résilience est beaucoup plus large et couvre à la fois la préparation à subir des attaques (prévention) et par-dessus tout à pouvoir continuer et reprendre une activité business normale très rapidement suite à une attaque, une catastrophe naturelle ou des incidents liés à la sécurité de l'information.

La sécurité n'est-elle donc pas suffisante. La sécurité vise à prévenir les incidents de sécurité et à gérer ces incidents mais ne prépare pas l'Organisation à faire face aux conséquences d'une cyberattaque et à récupérer ses aptitudes à créer de la valeur après en avoir été la victime.

Référentiels et normes

La cybersécurité pouvant être vue comme un sous ensemble de la cyber-résilience, il est clair que les référentiels et normes en matière de sécurité constitueront une première étape mais il convient d'élargir très sensiblement le périmètre pour couvrir les aspects de cyber-résilience.

Sécurité :

ISO 27001 – Systèmes de Management de la sécurité de l'information – Exigences

ISO 27002 – Code de bonne pratique pour le management de la sécurité de l'information

Cyber-résilience :

RESILIA – Bonnes pratiques de Cyber-Résilience

ISO 22301 – Systèmes de management de la continuité d'activité – Exigences

La cyber-résilience vise à gérer la sécurité en adoptant une approche globale impliquant à la fois les individus, les processus et la technologie. Elle impose une méthodologie à la fois solide et évolutive de gestion, d'analyse et d'optimisation des risques. Elle se pose comme le meilleur garant du capital informationnel des entreprises, organisations, États et individus.

La cyber-résilience s'appuie sur cinq piliers que sont la préparation/ l'identification, la protection, la détection, la résolution des problèmes et la récupération. Dans cette approche, il est donc essentiel de se poser les bonnes questions, d'adopter les bonnes mesures et de les réévaluer à un rythme régulier et de façon pragmatique, afin de gérer au mieux les cyber-risques.

Dès lors que les entreprises ont compris que les cyberattaques les affecteront tôt ou tard, indépendamment des efforts de prévention qu'elles auront mis en œuvre et seront couronnées de succès, elles peuvent passer à l'étape suivante : la conception et l'implémentation d'un Programme de Cyber-Résilience (PCR). Un PCR englobe bien sûr les concepts de défense et de prévention, mais va au-delà de ces mesures pour mettre l'accent sur la réponse et la résilience de l'organisation dans les moments de crise.

L'ILLUSOIRE SECURITE ECONOMIQUE DES ENTREPRISES

La notion de sécurité économique s'applique en premier lieu à la matérialisation d'une politique d'État visant à protéger et promouvoir les intérêts économiques stratégiques de la nation[33]. On peut parler alors de patriotisme économique aussi bien en défensif, c'est-à-dire en protégeant les intérêts économiques de la nation (et des entreprises) mais également en offensif, en accompagnant le développement à l'international des entreprises nationales.

L'objectif ici n'est pas d'aborder la sécurité économique au niveau étatique et les rapports de forces économiques qui découlent des volontés de suprématies de certains pays.

L'idée est de savoir si l'entreprise mondialisée peut être autonome voir indépendante dans la conduite de sa sécurité économique (réputation, protection de l'information stratégique, développement économique, ...).

Ce concept de patriotisme économique est plus ou moins mis en place par tous les pays, mais lorsque les deux plus grandes puissances mondiales que sont la Chine et les États-Unis l'utilisent de façon très agressive, les entreprises ciblées (et les pays) sont particulièrement vulnérables et démunies.

LES ARMES JURIDIQUES AMERICAINES POUR DOMINER L'ECONOMIE MONDIALE

Dans son livre sur ce sujet, Ali Laïdi[34] nous explique comment les États-Unis d'Amérique ont, au cours des vingt dernières années, mis en place tout un arsenal juridique au service de leur hégémonie économique. Les cibles : les entreprises étrangères (européennes principalement) qui sont concurrentes de leurs champions nationaux, dans le but de les affaiblir ou de les racheter.

Cela commence par la volonté de légiférer suite à :

- Un scandale touchant une entreprise américaine (corruption d'agent public à l'étranger, blanchiment d'argent, …).
- Un évènement susceptible de menacer la sécurité nationale (terrorisme, attentat du 11 septembre 2011, attaque dans le cyberespace).
- Un pays qui enfreint le droit et les libertés internationales (Cuba, Libye, Iran, Russie, …) d'un point de vue américain (en menaçant ses intérêts).

S'en suit une réponse sous plusieurs formes juridiques : soit une loi pour lutter contre la corruption d'agents publics étrangers, soit la mise en place de sanction ou d'embargo contre un pays, soit des lois qui sont de véritables « stratégies nationales » comme le *Patriot Act* ou le *Cloud Act*.

Si ces lois ont pour but premier de lutter contre le terrorisme, la corruption ou les régimes totalitaires (qui menacent la paix dans le monde…), elles sont combinées au formidable outil

[33] Cf. définition du Portail de l'IE : https://portail-ie.fr/resource/glossary/44/securite-economique
[34] Ali Laïdi, « Le droit, nouvelle arme de guerre économique » aux éditions Actes Sud, 2019

de renseignement américain pour sanctionner les entreprises étrangères qui seraient prises en faute (ou soupçonnées d'être en faute, selon le droit américain) partout dans le monde.

La force du système tient dans l'extraterritorialité de certaines de ces lois et elles s'appliquent donc à des personnes physiques ou morales de pays tiers, en raison de liens tenus avec les États-Unis (une filiale aux États-Unis ou un paiement en dollars). Les lois s'appliquent notamment à toutes les sociétés présentes sur les marchés financiers réglementés américains.

La question n'est pas la culpabilité des entreprises (ou des personnes) visées par ces lois mais bien de comprendre que ces lois sont au service d'un patriotisme américain particulièrement agressif et ciblé.

L'ARME ANTI-CORRUPTION

La lutte contre la corruption d'agents publics à l'étranger est incarnée par le *Foreign Corrupt Practices Act* (FCPA) de 1977 et qui a grandement influencé l'OCDE dans sa doctrine de lutte contre la corruption.

Deux agences sont chargées de faire respecter cette loi : Le DOJ « *Department Of Justice* », au pénal, qui poursuit les entreprises et les individus qui l'enfreignent et la SEC « *Security Exchange Commission* », au civil, qui s'attaque aux sociétés soupçonnées d'avoir falsifié leurs comptes.

L'extraterritorialité de cette loi est mise à profit par Washington pour sanctionner mais également pour attaquer les entreprises étrangères dans le but de les affaiblir.

Le cas d'Alstom est emblématique et très bien détaillé dans le livre de Frédéric Perruci[35]. Cet ex-haut dirigeant d'Alstom a payé de sa personne (plusieurs années de prison aux États-Unis) le patriotisme offensif américain à l'encontre de ce fleuron de l'industrie française et concurrent de l'américain General Electric (GE).

L'opération d'envergure menée par l'administration américaine pour que GE rachète une partie stratégique de l'entreprise française, fait l'objet actuellement d'une polémique politico-industrielle en France[36]. En effet, le calendrier de l'enquête du DOJ pour corruption d'une filiale d'Alstom, les pressions exercées sur les dirigeants et le rôle de l'État français sont au cœur d'une enquête parlementaire qui aboutira peut-être à la révélation d'un scandale sur la gestion de l'indépendance industrielle stratégique de la France *(cf. les Dépendances).*

La liste des entreprises européennes qui ont dû payer des amendes records au DOJ ne cesse de s'allonger. L'administration américaine tient même un site internet dédié[37] au FCPA pour promouvoir son action, comme l'illustre ce classement qui est régulièrement mis à jour :

[35] Frédéric Pierruci : « Le piège Américain » JC Lattés, Avril 2019
[36] Portail de l'IE : https://portail-ie.fr/short/2042/les-zones-dombre-de-laffaire-alstom-selon-frederic-pierucci
[37] http://www.fcpablog.com/

1. **Petróleo Brasileiro S.A. – Petrobras** (Brazil): $1.78 billion in 2018.

2. **Telia Company AB** (Sweden): $965 million in 2017.

3. **MTS** (Russia): $850 million in 2019.

4. **Siemens** (Germany): $800 million in 2008.

5. **VimpelCom** (Holland): $795 million in 2016.

6. **Alstom** (France): $772 million in 2014.

7. **Société Générale S.A.** (France): $585 million in 2018.

8. **KBR / Halliburton** (United States): $579 million in 2009.

9. **Teva Pharmaceutical** (Israel): $519 million in 2016.

10. **Keppel Offshore & Marine Ltd.**(Singapore): $422 million in 2017.

Figure 9 : Classement des 10 plus importantes amendes liées au FCPA

Ce qui frappe ici c'est la sous-représentation des entreprises américaines, alors que les européennes figurent en bonne place :

Entre 2008 et 2018, 26 sociétés ont réglé des pénalités de plus de 100 millions de dollars au trésor américain. Sur ces 26, 14 sont européennes, 5 sont françaises et 5 seulement sont américaines. Les sociétés européennes auront versé au total plus de 6 milliards de dollars et les américaines, trois fois moins. Les autorités s'en félicitent et s'en servent d'argument pour justifier leur action extraterritoriale. A elles seules les entreprises françaises ont déjà payé près de 2 milliards au titre du FCPA et au moins six de leurs cadres ont été mis en accusation par la justice américaine.

Mais ce qui est encore plus frappant c'est l'évolution des amendes. En 2004, le total des amendes payés par les entreprises au titre du FCPA était de 10 millions de dollars, en 2016 et 2017, elles ont explosé pour atteindre respectivement 2,7 et 1,9 milliards. Un grand bond en avant rendu possible par la promulgation du *Patriot Act* en 2003 (suite aux attentats de terroriste de 2001) qui a donné aux agences américaines (NSA, CIA, FBI) le droit d'espionner massivement les entreprises étrangères et leurs employés, sous couvert de lutte contre le terrorisme.

La prochaine entreprise européenne ciblée par le FCPA pourrait être Airbus, qui a tenté de « couper l'herbe sous le pied » des américains en se dénonçant aux autorités britanniques et françaises (pour une affaire de corruption). Mais cela ne pourrait peut-être pas suffire au DOJ, qui sous fond de difficulté de Boeing pourrait passer à l'offensif. D'autres entreprises sont sur la liste d'attente du DOJ et pour les européens (et la France) n'ont pas trouvé de solution (pour l'instant) contrecarrer l'extraterritorialité de cette loi. En effet rien ne prouve pour l'instant, que la loi (française) Sapin 2 et la récente création de l'agence française anticorruption (AFA) ne dissuadent les américains d'utiliser l'extraterritorialité du FCPA face aux entreprises françaises.

LES SANCTIONS ECONOMIQUES

Les États-Unis mettent en œuvre des sanctions économiques et des embargos au cas par cas contre des pays[38] qui enfreignent le droit international ou qui menacent leur sécurité nationale. La liste comporte plus d'une trentaine de pays et les sanctions sont diverses, mais les États-Unis imposent que tous les autres pays les suivent ! Ainsi, le Congrès américain a voté la loi CAATSA (*Counter America's Adversaries Through Sanctions Act* ou "Contrer les ennemis des États-Unis par le biais des sanctions") pour sanctionner la Russie. Cette loi impose des sanctions économiques contre toute entité ou pays, qui conclut des contrats d'armement avec des entreprises russes. Les États-Unis ont également rétabli les sanctions contre l'Iran et demandent au reste du monde de le respecter sous peine d'imposer des pénalités financières aux entreprises américaines et étrangères qui y contreviendraient. Malgré une tentative, la France et l'Europe n'ont pas vraiment trouver la parade pour continuer à commercer avec l'Iran et les groupes Français se sont retirés (une nouvelle fois) de ce marché (Total, Renault, Peugeot…) pour éviter tout problème avec l'administration US.

L'Office of Foreign Assets Control (OFAC), est le service du Trésor qui veille à l'application des sanctions internationales américaines dans le domaine financier, emploie environ 200 personnes et dispose d'un budget de plus de 30 millions de dollars pour détecter les transactions suspectes.

BNP Paribas s'est vu infliger en 2014 une amende de près de 9 milliards pour violation des sanctions internationales américaines (violations des embargos contre Cuba, l'Iran et le Soudan). Le DOJ a mis en avant la dimension de sécurité nationale, qui est l'une des justifications traditionnelles de l'extraterritorialité.
Fin 2018, c'est la Société générale qui a négocié une amende à près de 1,2 milliard d'euros après avoir effectué des transactions en dollars impliquant des pays sous le coup de sanctions américaines.

On comprend mieux pourquoi dans l'étude de PwC, c'est le secteur bancaire qui semble le mieux armé en termes de *compliance* et de *due diligence…*

Les entreprises françaises (Total, Technip, Alcatel, Alstom, Crédit Agricole, BNP, Société Générale…) ont payé plus de 13 milliards de dollars d'amende aux administrations américaines dans le cadre de ces lois extraterritoriales (FCPA, embargos etc…) alors qu'elles auraient pu être payées aux administrations des pays concernés par la « fraude » ou encore à la France…

L'HEGEMONIE SUR LE COMMERCE MILITARO-INDUSTRIEL

Pour lutter contre le trafic d'armes les États-Unis ont mis au point une régulation : ITAR (*International Traffic in Arms Regulations*).

Si un système d'armes contient au moins un composant américain sous le régime de la réglementation ITAR, les États-Unis ont le pouvoir d'en interdire la vente à l'export à un pays

[38] Liste des pays : https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx

tiers. Les américains se servent d'ITAR pour arbitrer le marché mondial de l'armement, dont ils sont les leaders.
Or beaucoup de sociétés françaises et européennes intègrent des composants américains notamment électroniques, dans de nombreux matériels, tout particulièrement dans les domaines aéronautique et spatial. "Notre dépendance à l'égard des composants soumis aux règles ITAR est un point critique", avait reconnu en mai 2011 à l'Assemblée nationale le PDG de MBDA, Antoine Bouvier.
Washington a récemment interdit l'exportation du missile de croisière Scalp de MBDA vers l'Égypte et le Qatar (ce qui freine la vente de Rafale supplémentaires au Caire). Au-delà du camouflet économique, c'est clairement une atteinte à la souveraineté de la France et ce n'est pas la première fois que cela se produit.
Certains dossiers imposent au pays des négociations au plus haut niveau. Ce fut le cas en 2013 quand ils avaient refusé une demande de réexportation aux Émirats Arabes Unis de composants « made in USA » nécessaires à la fabrication de deux satellites espions français (fait par Airbus et Thales). La visite de François Hollande aux États-Unis en février 2014 avait permis de régler positivement ce dossier mais on ne connait pas les contreparties de cet accord…

LE CONTROLE DES INVESTISSEMENTS ETRANGERS

L'administration américaine, sous l'impulsion du président Donald Trump, a encore durci les conditions d'investissement étranger dans les sociétés américaine disposant de technologies sensibles. La réforme du Comité sur les investissements étrangers (*Committee on Foreign Investment in the United States*, CFIUS) adoptée à l'été 2018, va exiger des investisseurs étrangers qu'ils soumettent obligatoirement aux autorités toute prise de participation dans une entreprise américaine appartenant à l'un des 27 secteurs clés désignés, dont l'aéronautique, les télécoms, l'industrie informatique, celle des semi-conducteurs et des batteries. L'administration Trump préparerait d'autres réglementations pour les domaines de l'intelligence artificielle et des infrastructures.

C'est une mesure de patriotisme économique défensif qui protège les entreprises américaines mais qui peut fragiliser les entreprises étrangères dans les domaines très concurrentiels. En effet, tout le monde ne joue pas avec les mêmes règles dans le grand jeu de la mondialisation.

LE PROTECTIONNISME COMMERCIAL

La recrudescence des mesures protectionnistes est l'un des risques majeurs pour les échanges commerciaux mondiaux et donc pour les entreprises mondialisées. Ces dernières années, l'administration des États-Unis est la plus active dans ce domaine, symbolisé par le bras de fer avec la Chine sur les droits de douane des importations chinoises.

C'est une arme de politique extérieure utilisée sans limite par Donald Trump et quasiment aucun pays n'échappent à la menace. En juin 2019, le Mexique a dû prendre des mesures fortes pour freiner le flux de migrant traversant le pays suite à la menace d'une augmentation des tarifs douaniers vers les États-Unis.

Ces mesures sont évidemment au cœur des enjeux de puissance entre les pays et à ce jeu-là, les américains ont une longueur d'avance sur le reste du monde et notamment l'Europe. Mais les victimes de ces guerres économiques sont en premier lieu les entreprises touchées par ces mesures.

Le meilleur exemple est le géant chinois des nouvelles technologies Huawei. Huawei s'est retrouvé la principale victime de la guerre pour le leadership économique et technologique mondial mené par les États-Unis face au Chinois. Ils ont réussi le tour de force de faire bannir cette entreprise dans la plupart des pays occidentaux en quelques mois, une fois de plus sous prétexte de sécurité nationale *(cf. les Dépendances)*.

LE CLOUD ACT

Parfois présenté comme la réponse américaine au RGPD européen, le *Cloud Act* (*Clarifying Lawful Overseas Use of Data Act*) est une loi fédérale américaine promulguée le 23 mars 2018 bien plus offensive en termes de sécurité, de souveraineté numérique et de patriotisme économique. Elle permet désormais aux forces de l'ordre ou aux agences de renseignement américaines d'obtenir des opérateurs télécoms et des fournisseurs de services de *Cloud computing* des informations stockées sur leurs serveurs, que ces données soient situées aux États-Unis ou à l'étranger. Les grands acteurs américains du cloud et leurs filiales devront donc s'y conformer. Tout comme le devront les autres entreprises du secteur, y compris européennes, qui opèrent sur le territoire américain.

Avec le *Patriot Act*, le *Cloud Act* est une mesure supplémentaire pour garantir la sécurité nationale des États-Unis contre le terrorisme. C'est également un formidable outil pour permettre aux agences de renseignements de « légaliser » leurs tâches d'espionnage tout azimut et notamment l'espionnage économique.

La protection du patrimoine immatérielle des entreprises va devenir un vrai challenge pour les entreprises mondialisées, tant les entreprises américaines (et chinoises) dominent le flux et le stockage des données mondiales *(cf. les Dépendances).*

LES DEPENDANCES ECONOMIQUES

Les entreprises, conscientes ou malgré elles, sont soumises, tout au long de leur vie, à des dépendances qui, à un moment ou un autre, sont susceptibles de mettre en péril leur intégrité.

Les dépendances auxquelles font face les entreprises sont multiples et protéiformes, aussi bien externes qu'internes. Il peut très bien s'agir d'une dépendance envers un État, comme nous allons le voir avec l'exemple récent des États-Unis et de Huawei. Mais la dépendance peut provenir aussi d'une entreprise : fournisseurs, clients, sous-traitants, prestataires de services.

Au sein même de l'entreprise, la dépendance pourra revêtir un autre visage : la société pourra être totalement tributaire de son PDG ou d'un employé au talent rare et au savoir-faire indispensable.

S'il est impossible de lister et de présenter de manière exhaustive toutes les dépendances entourant une organisation, nous nous attacherons à illustrer les dangers pour une entreprise et montrerons dans quelles mesures la dépendance à un État, aux géants du numérique ou à des consultants externes (par exemple, les cabinets d'avocats des Big 4) peut être toxique.

SOUS L'OMBRE DES ÉTATS

Nous avons abordé en préambule la position des États-Unis qui, au nom de leur sécurité nationale ou sous prétexte de lutter contre la corruption, vont chercher à affaiblir ou faire plier une entreprise stratégique étrangère susceptible d'acquérir un marché ou de supplémenter sa concurrente américaine. Une manœuvre savamment orchestrée avec comme premiers bénéficiaires, les sociétés américaines.

La coopération public/privé aux États-Unis est une relation solide avec de vrais enjeux stratégiques mais la Chine n'est pas en reste en reste en la matière. Ces deux États ont un même leitmotiv : Derrière une entreprise florissante se cache un État fort.
La domination actuelle des États-Unis est telle qu'une action du gouvernement américain engendre des répercussions au niveau mondial. Ces dernières peuvent être néfastes pour l'économie mondiale et susceptibles de mettre en danger aussi bien l'équilibre des entreprises américaines, européennes ou asiatiques.
Derrière les enjeux politiques et économiques globaux qui se jouent entre les États, nous nous intéresserons aux conséquences directes que peuvent avoir les actions étatiques sur les entreprises qui se retrouvent bien souvent positionnées sur l'échiquier.

Obnubilés par l'« *America first* » et par crainte de voir la Chine truster la première place au classement des puissances mondiales, qui lui semble désormais acquise dans une dizaine d'années selon les projections (voir tableau ci-dessous « Classement des principaux pays par PIB »), les États-Unis sont entrés dans une guerre commerciale contre elle. Dans cette guerre froide 2.0, une des victimes collatérales se nomme Huawei. En effet, depuis plusieurs mois, Donald Trump accuse le fabricant chinois d'équipements télécoms et de smartphones de servir à des activités d'espionnage pour le compte du gouvernement chinois au travers de ses équipements.

	2017	2018	2022	2027	2032
U.S.	1	1	1	1	2▼
China	2	2	2	2	1▲
Japan	3	3	3	4▼	4
Germany	4	4	4	5▼	5
India	7	5▲	5	3▲	3
France	5	6▼	7▼	8▼	9▼
U.K.	6	7▼	6▲	6	7▼
Brazil	8	8	8	7▲	6▲
Italy	9	9	9	12▼	13▼
Canada	10	10	11▼	10▲	12▼
South Korea	12	12	10▲	9▲	8▲
Indonesia	16	16	16	13▲	10▲

Source: Centre for Economics and Business Research — Bloomberg

Figure 10 : Classement des principaux pays par PIB

La marque chinoise va alors faire face à des intimidations, des menaces et des actions prises contre elle, comme entre autres, la promulgation d'une loi, en août 2018, interdisant aux autorités fédérales américaines de recourir aux équipements de Huawei et d'un autre groupe chinois, ZTE mais aussi le 1er décembre 2018, l'arrestation, au Canada, de Meng Wanzhou, directrice financière de la société Huawei et fille du fondateur de l'entreprise, à la demande des États-Unis pour fraudes supposées envers plusieurs institutions financières, en violation des interdictions imposées par les États-Unis de traiter avec l'Iran.

Huawei et ses filiales sont également placés sur une liste noire[39] élaborée par Washington qui répertorie les sociétés, considérées comme « à risque » pour la sécurité nationale américaine, qui « créent et exploitent de plus en plus de vulnérabilités dans le domaine des technologies et des services de l'information et des communications […] afin de commettre des actes cyber-malveillants, notamment l'espionnage économique et industriel contre les États-Unis et son peuple »[40].

Enfin, Donald Trump signe, le 15 mai 2019, un décret hostile à Huawei, demandant à toutes les entreprises américaines de cesser d'approvisionner et de collaborer *avec* l'entreprise chinoise. Une mesure qui pourrait provoquer un fort ralentissement voire la possible disparition de l'actuel numéro deux mondial du marché des smartphones *et* également leader mondial des équipements 5G, déjà interdit sur le marché américain.

Cette ultime attaque contre Huawei, fierté nationale et fleuron de l'industrie chinoise a des impacts sur deux univers distincts, sur le marché des smartphones et sur celui des équipements de télécommunications 5G mais aussi sur les acteurs de ces segments.

La répercussion sur le marché des smartphones

Le marché des smartphones est devenu, l'année passée, le principal générateur de revenus de Huawei, grâce notamment à une forte croissance en Europe et en Asie. La bonne santé de cette branche se faisait encore ressentir jusqu'au trimestre dernier, avant l'annonce de la signature du décret défavorable à Huawei.

D'après le dernier rapport du cabinet IDC, datant de mai 2019, les ventes de smartphones de Huawei dans la zone EMEA (Europe, Moyen-Orient et Afrique), au cours du premier trimestre 2019, progressaient de 66,13% quand Apple et Samsung enregistraient une perte de vitesse, leurs ventes reculant respectivement de 22,73% et 6,82%.

Si Samsung conservait la première place du classement avec 29,47% des parts de marché, Huawei dépassait Apple pour se retrouver en deuxième position avec 25,39% des parts de marché contre 14,74% pour la marque à la pomme reculant à la troisième du podium.

[39] http://www.lefigaro.fr/secteur/high-tech/outre-huawei-quels-sont-les-groupes-chinois-sur-la-liste-noire-de-donald-trump
[40] https://www.numerama.com/donald-trump-exclut-huawei-des-telecoms-aux-usa-au-nom-de-lurgence-nationale.html

Company	2018Q1 Unit Shipments	2018Q1 Market Share	2019Q1 Unit Shipments	2019Q1 Market Share	2019Q1 Unit YoY Growth
Samsung	16.9	30.76%	15.7	29.47%	-6.82%
Huawei	8.1	14.86%	13.5	25.39%	66.13%
Apple	10.2	18.55%	7.8	14.74%	-22.73%
Xiaomi	2.2	4.05%	2.9	5.55%	33.26%
HMD	3.3	6.08%	2.2	4.21%	-32.64%
Others	14.1	25.69%	11.0	20.64%	-21.86%
TOTAL	55.0	100%	53.5	100%	-2.74%

Source: IDC Quarterly Mobile Phone Tracker, May 2019

Figure 11 : Ventes de smartphones en zone EMEA, au 1er trimestre 2019

Mais il faudra surveiller avec attention les chiffres des prochains mois qui permettront de mieux jauger l'impact du décret émis par les américains et de constater à quel point la dynamique de Huawei pourrait être brisée, alors que le chinois était en passe de supplanter Samsung en termes de ventes et de lui ravir la première place du marché des smartphones.

Pour l'heure, un ralentissement des ventes du chinois a déjà été constaté en France et en Espagne, dans les semaines qui ont suivi l'annonce.

De toute évidence, cela fera très certainement les affaires d'Apple et Samsung qui pour l'un retrouvera sa place de numéro deux et pour l'autre conservera sa position de leader dans la zone EMEA.

La signature du décret a pour effet la désaffection d'un grand nombre de sociétés qui travaillaient jusqu'alors avec Huawei et marque la fin de leur collaboration. Ces désengagements en cascade sont contraints et s'expliquent par le fait qu'une entreprise, quelle que soit sa nationalité, qui vendrait aux chinois des composants qui intégreraient de la technologie américaine, tomberait sous le coup du décret de Donald Trump et devrait alors subir le courroux des États-Unis et de sa justice.

La première entreprise à annoncer la rupture est Google. L'exécutif américain donne trois mois (délai accordé au chinois pendant lequel une partie des sanctions prononcées à son encontre ne sont pas appliquées) à Google et Huawei pour organiser et acter leur divorce.

Google cesse donc d'approvisionner Huawei et ne fournira plus ni logiciels, ni matériels, ni services techniques sur les futurs smartphones fabriqués par le chinois, exception faite des services disponibles en « open source ». Adieu l'écosystème à succès de la marque américaine, où tout est réuni pour proposer une expérience client unifiée, avec des applications comme Gmail, Chrome, Google Maps, YouTube, terminé la possibilité d'intégrer *Play Store* (magasin virtuel permettant d'accéder à des millions d'autres applications et leur

mise à jour). Et surtout cela sonne la fin de l'exploitation d'Android, l'OS[41] qui fait tourner près de 9 smartphones sur 10 dans le monde[42].

Quelques jours après Google, le couperet tombe cette fois chez Facebook. Il n'autorise plus, à partir du 7 juin 2019, la pré-installation de ses applications (Facebook, Instagram, WhatsApp, Messenger,…) sur les smartphones du chinois se trouvant encore sur les lignes de production ou les nouveaux à venir[43].

Pour mesurer l'impact de l'annonce de Google, qu'il se plierait à la décision de Washington, sur les entreprises qui collaborent avec Huawei, il suffit de regarder vers les cours de Bourse des fabricants de semi-conducteurs européens pour constater la répercussion immédiate sur ces derniers. Le 20 mai, en France, deux spécialistes des semi-conducteurs, STMicroelectronics et Soitec, étaient lourdement affectés, leurs actions perdant respectivement 9,50% et 7,20% à la clôture[44].

Il est à noter que Huawei fait partie parmi les dix clients plus gros de STMicroelectronics[45] et que Soitec est en relation indirecte avec le chinois, par l'intermédiaire d'au moins deux de ses premiers clients : NXP Semiconductors, qui classe lui aussi Huawei parmi ses dix premiers clients et STMicroelectronics. Sur l'exercice 2017-2018, les cinq premiers clients de Soitec représentent 57% de son chiffre d'affaires[46].

Cette dépendance à ses cinq plus gros clients, dont deux sont directement liés à Huawei, doit pousser Soitec à s'inquiéter sur sa capacité à absorber le trou d'air que générera l'arrêt du partenariat de Huawei avec ses clients.

Le fabricant américain de semi-conducteurs Broadcom a indiqué, le 13 juin, dans un communiqué de résultats, avoir revu à la baisse son chiffre d'affaires prévisionnel pour 2019, préférant adopter « une position conservatrice pour le reste de l'année », « en raison d'une faiblesse généralisée de la demande liée au contexte d'incertitudes géopolitiques et à l'impact des restrictions à l'export imposées au chinois Huawei, l'un de ses principaux clients. »[47]

A la suite de cette annonce, le titre de la société reculait de 7,1% à la clôture.

Huawei subit également une vague d'annulations de commandes pour ses nouveaux smartphones de la part d'opérateurs télécoms comme les britanniques EE et Vodafone, les japonais NTT Docomo, KDDI et YMobile mais aussi le taïwanais Chunghwa Telecom[48].

Encore plus grave, Huawei est surtout abandonné par les fabricants de composants comme les américains AMD, Intel, Qualcomm, l'allemand Allemand Infineon et l'anglais ARM.

Collaborer avec ARM est hautement stratégique et primordial puisque la société est à l'origine de l'architecture de tous les processeurs pour smartphones dans le monde. En clair, à l'heure actuelle, sans ARM, pas de téléphones.

[41] Operating System. En français, système d'exploitation
[42] Sur les 344,3 millions de smartphones livrés dans le monde au 2e trimestre 2016, 86,2% étaient sous Android selon Gartner Inc.
[43] https://www.reuters.com/article/us-huawei-tech-usa-facebook/facebook-suspends-app-pre-installs-on-huawei-phones
[44] https://www.lerevenu.com/bourse/huawei-dans-la-tourmente-soitec-et-stmicro-trinquent-en-bourse-nokia-en-profite
[45] https://fr.reuters.com/article/frEuroRpt/idFRL5N22W11U
[46] https://www.soitec.com/media/upload/1_assemblee_generale/20180726_AGOE_VF/Soitec-DDR-2017-2018-VFfinale.pdf
[47] https://fr.reuters.com/article/businessNews/idFRKCN1TE36A-OFRBS
[48] https://www.tomsguide.fr/huawei-la-liste-des-deserteurs-sallonge/

Huawei qui justement s'enorgueillissait d'avoir le contrôle de ses propres processeurs Kirin avec son partenariat avec ARM et de ne plus dépendre de l'américain Qualcomm pour faire tourner ses smartphones, va devoir rapidement trouver de nouvelles alternatives. Car si le processeur qui équipera le prochain modèle haut de gamme est déjà conçu et n'est pas concerné par le véto américain, ARM ne fournira plus les prochaines puces à la marque chinoise. Ce qui pourrait remettre fortement en cause l'ensemble des productions des smartphones Huawei à venir.

Pour survivre sans ARM, Huawei devra tourner vers de nouveaux fournisseurs asiatiques ou étrangers prêts à travailler avec lui et dont les composants ne comportent aucune technologie américaine. Huawei pourrait également entreprendre de développer sa propre architecture, ce qu'aucun grand constructeur n'a réalisé jusqu'ici mais la tâche s'annonce complexe dans un laps de temps aussi court.

Les conséquences économiques pour les fournisseurs américains de Huawei

Huawei n'est pas le seul à subir sa mise à l'écart du marché américain, nombre d'entreprises américaines sont également pénalisées, tant les économies américaines et chinoises sont interdépendantes en matière de nouvelles technologies et tant Huawei est omniprésent sur ces marchés.

Dans une étude, Goldman Sachs, la banque d'investissement américaine, fait apparaître les entreprises américaines pour lesquelles la sanction américaine aura le plus de répercussions, leurs revenus provenant pour grande partie de leur partenariat avec Huawei.

Le graphique « Revenue from Huawei » (à gauche) montre les revenus réalisés par chaque fournisseur de Huawei grâce à leur collaboration. Le graphique « Most exposed » (à droite), lui, met en évidence la part que représente Huawei sur les revenus totaux de chaque fournisseur. Le but étant de mesurer l'impact de l'éviction de Huawei, le degré de dépendance des fournisseurs par rapport au chinois et leur capacité à résister à la perte de ce dernier.

Nous pouvons constater, grâce au graphique « Revenue from Huawei », que c'est la société Flex, une entreprise spécialisée dans la sous-traitance de composants électroniques, qui avec environ 351 millions de dollars[49], génère le plus de revenus grâce à Huawei. Suivent Broadcom (302 millions $US), Qualcomm (228 millions $US), Seagate Technology (120 millions $US), Micron Technology (111 millions $US), Qorvo (94 millions $US) et Intel (85 millions $US), qui dégagent les plus gros revenus et seront les plus marqués par le bannissement de Huawei. AMD sera impacté à hauteur d'environ 39 millions de dollars.

D'après l'histogramme « *Most exposed* », c'est la société Neophotonics, développant des produits pour réseaux de communication, qui devrait le plus pâtir de la perte de Huawei, la marque chinoise représentant environ 47% de ses revenus globaux. Une telle dépendance à un client, qui cesse son activité sur le territoire états-unien, pourrait être fatale à l'entreprise américaine. Par contre, la fin du partenariat avec Huawei n'aura qu'une faible incidence pour des entreprises de plus grande renommée comme Broadcom (6%), Qualcomm (5%), Intel (1%) et Microsoft (N/S) qui ont des revenus plus diversifiés.

Les sanctions contre Huawei pourraient toucher plus particulièrement les plus petites entreprises, moins résilientes, comme Corning, qui fabrique un verre ultrarésistant pour

[49] Taux de conversion Yuan/Dollar au 15 juin 2019

smartphone, dont les revenus issus du partenariat avec Huawei s'élèvent à 53 millions de dollars. Pour Lumentum Holdings, société spécialisée dans l'optique et le laser, Huawei représente 11% de son chiffre d'affaires.

Roger Kay, analyste chez Endpoint Technologies, estime qu'« à court terme, l'effet est inévitablement négatif pour les entreprises américaines et chinoises» mais qu'« à plus long terme, le résultat, c'est que Huawei et les autres groupes chinois vont se détourner davantage des fournisseurs américains. »[50]

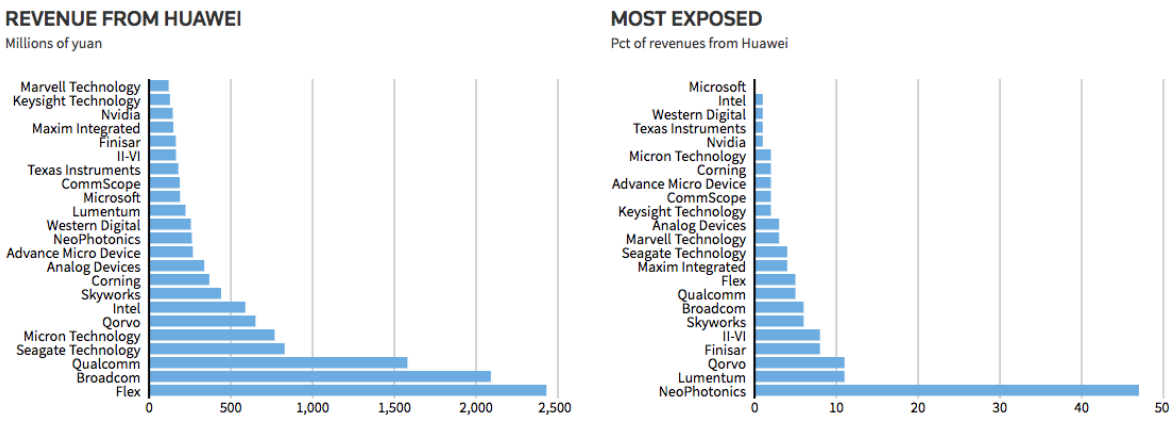


Figure 12 : Revenus et pourcentage des revenus issus de Huawei

Dans son étude, Goldman Sachs indique également l'origine des fournisseurs de Huawei. Ainsi, 30% d'entre eux proviennent de Chine et 23% sont américains. C'est quasiment un quart des fournisseurs, sans compter les fournisseurs étrangers dont les produits contiennent de la technologie américaine, qu'il faudra remplacer. Cela marque la forte dépendance du chinois pour la technologie et les solutions américaines. Un autre problème épineux pour lequel le constructeur chinois devra rapidement trouver une solution.

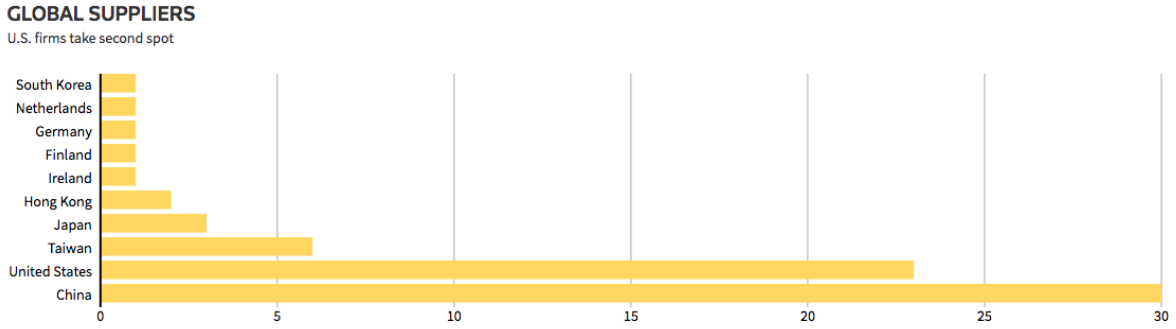


Figure 13 : Principaux fournisseurs de Huawei (par pays)

Source : Goldman Sachs citing company data, Bloomberg[51]

[50] https://www.mesactions.com/economie-et-finances/les-groupes-americains-aussi-font-les-frais-des-sanctions-contre-huawei
[51] https://fingfx.thomsonreuters.com/gfx/editorcharts/USA-CHINA-HUAWEI/0H001GSE93H2/index.html

Les réactions de la Chine et de Huawei suite à l'éviction de ce dernier

La Chine n'a pas tardé à réagir en apprenant l'éviction de Huawei, Xi Jinping, le président chinois, a rappelé que son pays avait un quasi-monopole sur la production des terres rares comme le tantale, le cobalt, et le tungstène, éléments stratégiques et essentiels pour les nouvelles technologies. La Chine pourrait, en mesure de représailles, interdire l'exportation de ces minéraux. Ces métaux font d'ailleurs partie des rares produits chinois exclus de taxes douanières américaines, signe de l'attrait que leur portent les américains.

Dans son discours, Xi Jinping s'est montré ferme en indiquant que la Chine avait les ressources nécessaires pour lutter contre les États-Unis et « la guerre commerciale ne mettra pas la Chine à genoux » mais qu' « elle ne fera que [les] endurcir pour croître encore plus. »

En plus de la menace sur les terres rares, le gouvernement chinois a annoncé qu'il établirait et publierait également une liste noire « d'entreprises, organisations et particuliers étrangers » jugés « non fiables »[52]. Une mesure qui pourrait toucher les entreprises avec lesquelles Huawei collaborait. Mais elle pourrait surtout affecter Apple qui représente 8,4% du marché chinois des smartphones, soit 34,2 millions d'unités vendues en 2018[53]. Un tel scénario, selon une étude de Goldman Sachs, pourrait causer à la marque à la pomme la perte de près d'un tiers de ses profits[54].

Ren Zhengfei, le fondateur de Huawei, a indiqué dans un entretien à Bloomberg que des représailles de Pékin contre Apple étaient peu probables et que si cela devait arriver, il s'opposerait à de telles mesures.

Le PDG a confirmé que son entreprise avait la capacité de concevoir ses propres solutions et que Huawei élaborait ses propres processeurs depuis des années, utilisés sur un bon nombre de ses propres smartphones mais surtout qu'il avait développé son propre système d'exploitation. Mais le dirigeant chinois a éludé la question concernant le temps nécessaire à la mise en œuvre de ces solutions alternatives en déclarant non sans humour que « cela dépendra de la rapidité avec laquelle [leurs] réparateurs seront en mesure de réparer l'avion, quels que soient les matériaux utilisés, qu'il s'agisse de métal, de tissu ou de papier, l'objectif est de maintenir l'avion dans les airs. ».

Le chinois a ainsi anticipé la situation dans laquelle il se trouve et a passé les dernières années à développer son système d'exploitation maison, nommé ArkOS. Mais le constructeur n'est pas pressé de le lancer puisqu'il a toujours des accords avec Google courant jusqu'à août 2019.

Dans un communiqué, Huawei a indiqué avoir « contribué fortement au développement et à la croissance d'Android dans le monde et en tant que partenaire mondial d'Android » et a travaillé « étroitement avec sa plateforme open source pour développer un écosystème qui profite à la fois aux utilisateurs et à l'industrie ». C'est sur cette base qu'ArkOS devrait tourner.

La réponse de Huawei à l'offensive de Washington est donc l'exploitation prochaine de son propre OS mais qui devra reposer sur une nouvelle architecture de processeurs. Si tant bien que mal Huawei semble résister aux attaques des États-Unis et pourrait se défaire d'une

[52] https://www.ledevoir.com/economie/555786/guerre-commerciale-la-chine-sort-une-liste-noire-d-entreprises-non-fiables
[53] https://www.zdnet.fr/actualites/les-consommateurs-chinois-ont-boude-l-iphone-et-d-autres-smartphones-39879847.htm
[54] https://www.bloomberg.com/news/articles/2019-05-22/apple-earnings-could-be-slashed-29-on-a-china-ban-goldman-says

dépendance américaine, la guerre est loin d'être remportée. La charge américaine a malgré tout ébranlé le géant chinois et les prochains mois seront déterminants en fonction des stratégies adoptées et des nouveaux partenariats liés.

Avec ArkOS, Huawei se mettra à l'abri de toute interdiction américaine mais ne se sauvera pas totalement. Car la firme chinoise devra rivaliser avec des écosystèmes bien implantés, que sont Android de Google et iOS d'Apple, et proposer un produit suffisamment élaboré et attractif, avec en plus d'une boutique virtuelle riche en applications. D'ailleurs sans accès au Play Store, la firme chinoise s'est déjà lancée dans la course aux développeurs et incite ces derniers à rejoindre sa propre boutique en vantant l'attrait de l'écosystème Huawei, et en offrant sa coopération et son aide à ceux qui voudraient développer pour sa « App Gallery ».

Les États-Unis se sont peut-être rendus compte trop tard qu'il ne fallait pas sous-estimer Huawei. Les BATX ont su brillamment exister face aux GAFA, il y a sûrement une véritable occasion pour les chinois de fabriquer un véritable concurrent à Google et Apple au niveau mondial. En attendant cela signifie que la marque chinoise devra proposer des produits pour lesquels les consommateurs devront se passer des écosystèmes de Google et Apple auxquels ils tiennent aujourd'hui et c'est en cela un véritable challenge technologique et commercial.

Un résultat à l'inverse de l'objectif escompté par Trump ?

Dans une interview accordée à The Mail On Sunday, Hermann Hauser, le fondateur d'ARM (fabricant anglais de semi-conducteurs) est revenu sur les conséquences du décret de Donald Trump qu'il critique et prédit des « dégâts énormes » pour son entreprise et l'industrie américaine en général.

Hermann Hauser estime que « tous les fournisseurs dans le monde commenceront à vouloir réduire la menace d'une production entièrement dépendante du président américain ». Il affirme avoir des discussions avec « des entreprises en Europe confirment le fait qu'elles analysent leur portfolio de propriétés intellectuelles afin d'écarter tout ce qui américain ». De telle sorte que ces entreprises européennes n'auraient plus à se plier à la politique américaine.

Le fondateur avoue qu'ARM réfléchirait à se libérer également des technologies américaines, « la plupart des propriétés intellectuelles d'ARM ont été conçues en Europe, mais certaines d'entre elles, sans qu'[ils en soient] conscient[s], ont été créées aux États-Unis » et « beaucoup de produits ARM sont composées de propriétés intellectuelles américaines », ce qui contraint donc ARM à « obéir aux ordres du président américain » et que regrette l'homme d'affaires qui qualifie la situation d'inacceptable.

Durant l'entretien, Hermann Hauser s'interroge sur le fait que « si les États-Unis peuvent arrêter une entreprise chinoise, ils peuvent bien entendu arrêter n'importe quelle entreprise dans le monde. En exerçant leur incroyable pouvoir sur d'autres entreprises, toutes les firmes du monde se demandent : Est-ce que je veux être dans une position où le président américain puisse me fermer boutique ? » Il précise aussi que pour éviter de se retrouver sous pareille situation « les personnes de l'industrie font très attention à ne pas acheter de produits américains. »[55]

[55] https://www.phonandroid.com/huawei-lexclusion-du-constructeur-va-faire-des-degats-enormes-estime-arm.html

Un décret qui se voulait protectionniste envers les entreprises américaines pourrait finir par conduire à un boycott des technologies américaines par le reste du monde.

Google se montre également inquiet quant aux conséquences de ce décret et s'est efforcé de démontrer à Washington qu'il ne s'agissait pas de la meilleure position à adopter. Le géant américain avance qu'en contraignant Huawei à abandonner Android et à développer son propre OS, ArkOS, probablement conçu à partir de la version open source d'Android (AOSP), cela l'empêchera d'avoir une visibilité sur ce qu'il se passe sur le système d'exploitation chinois.

Google suppose que l'OS de Huawei sera forcément moins sécurisé qu'Android et davantage susceptible d'être piraté, dans la mesure où il fournira plus Google Play Protect. Ce dernier est l'outil de protection maison « qui regroupe des outils de sécurité fonctionnant avec Android et qui permet de se protéger des menaces provenant d'applications non vérifiées, frauduleuses ou tout simplement dangereuses ». Les applications qui figureront sur le « App Gallery » de Huawei ne passeront plus les contrôles préalables que Google réalise habituellement permettant de faire le ménage fréquent et de limiter les risques de malwares.

Enfin, Google ne doute pas que Huawei finira par réussir à vendre par millions ses smartphones malgré un nouvel écosystème. Des informations sensibles seront alors partagées entre smartphones Android de Google et ArkOS de Huawei. Sauf que les données qui s'échangeront, avec les appareils du chinois (potentiellement moins bien protégés, déjà infectés ou espionnés) pourront être exposées ou interceptées par des tiers mal intentionnés mettant ainsi en péril… la sécurité nationale américaine.

Le président Trump a peut-être changé l'avenir du monde des smartphones. Sans son intervention, Huawei aurait pu s'en tenir à l'écosystème de Google. Mais aujourd'hui, le chinois n'a pas d'autre choix que de lutter et de contester la domination de Google et d'Apple pour assurer sa propre survie.

Google a bien compris l'intérêt de continuer à collaborer avec le groupe chinois, économiquement d'abord mais aussi parce que son leadership pourrait être remis en cause. C'est donc également pour des raisons stratégiques qu'il a demandé à l'administration Trump d'autoriser de nouveau l'exploitation d'Android à Huawei. Mais même si l'exécutif américain décidait de lever l'interdiction dans le cadre d'un accord commercial, Huawei semble désormais résolu à avancer de manière indépendante et autonome.

Donald Trump, en maintenant sa politique protectionniste et en se lançant aveuglement dans une guerre commerciale contre la Chine, n'a peut-être envisagé un seul instant que ses actions pourraient se retourner contre les États-Unis eux-mêmes. Le président américain a non seulement porter préjudice économiquement à de nombreuses entreprises américaines mais a aussi contribué à accentuer le fossé existant entre l'Internet « made in America » et celui « made in China ». Et il a surtout entamé la capacité des géants américains de la technologie, que sont Google et Apple, à maintenir leur domination face à l'ogre chinois.

SOUS LA COUPE DES CABINETS D'AVOCATS D'AFFAIRES ANGLO-SAXONS

Conformité / Juridique

La conformité est un enjeu majeur pour les entreprises en raison des conséquences pénales, financière et de réputation. Elle regroupe un ensemble de processus qui permettent d'assurer le respect des normes, règlementations et conventions applicables à l'entreprise. Ces dernières années, les scandales de non-conformité ont prouvé les conséquences terme de préjudice pour l'entreprise. Aujourd'hui elle se trouve au cœur de la gouvernance et des en enjeux stratégiques de l'entreprise et doit en effet faire partie du scope de la sécurité globale de l'entreprise.

Le marché de la compliance qui est né aux États-Unis en ont fait un business mondial comme pour tout. En France comme en Europe, le marché en conformité (cabinets d'avocats, cabinets d'audits, cabinet d'avocat d'affaires) est accaparé en grande partie par des sociétés américaines[56]. Sauf qu'il est ici question de sécurité économique, nationale et de souveraineté économique.

Selon Christian Harbulot, :

« *Les grands groupes français ont pris l'habitude de consulter les cabinets à dominante nord-américaine, créant ainsi une dépendance durable et fortement préjudiciable à nos intérêts économiques* ». [57]

« La définition des normes était un premier signal d'alerte entrevu au début des années 90. Trente ans après, l'occupation offensive du terrain s'est élargie à de nombreux domaines : gestion du risque financier, respect de la conformité, discours sur la lutte anticorruption, sécurisation des moyens de paiement bancaire »

Il évoque également que :

« *La matière juridique n'est pas une production neutre de connaissances. Elle est même devenue un enjeu majeur dans la manière de prendre l'avantage sur ses adversaires* »

« Nous avons laissé les anglo-saxons formater et conquérir le marché mondial du droit des affaires. Les conséquences ne sont pas négligeables »

Les États-Unis sont les champions du monde en matière de soft power, ils ont toujours exercé un pouvoir d'influence considérable sur une partie de l'administration, de l'économie et de la classe politique française, nos élites politiques sont bien plus atlantistes qu'on ne le pense.

Chaque année depuis 1945 l'ambassade des États-Unis à Paris identifie les futures élites françaises puis les invite à Washington pendant plusieurs semaines dans le cadre d'un programme baptisé Young leaders.

[56] https://www.magazine-decideurs.com/classements/compliance-programmes-de-conformite-classement-2018-cabinet-d-avocats-france-1
[57] https://infoguerre.fr/2019/04/guerre-economique-question-essentielle-encerclements-cognitifs/

Gouvernance de l'Internet

L'internet est un réseau généraliste, qui n'est pas dédié à un usage unique.

La « gouvernance de l'internet », fonctionne selon un schéma « multi-acteurs » associant les États, les sociétés civiles, les entreprises et les organismes à vocation internationale. L'Internet « *Corporation for Assigned Names and Numbers (Icann18)* » et l'Internet *Engineering Task Force* (IETF) définissent une partie de ces aspects techniques que sont les protocoles du réseau, conjointement avec le *World Wide Web Consortium (W3C)*, en charge des standards du web.

Voilà plusieurs décennies que la prééminence américaine, garante supposée d'un réseau unique, ouvert et décentralisé, est largement contestée, revendiqué le « droit souverain » des gouvernements à « réguler le segment national de l'internet »

L'architecture de l'Internet est devenue à la fois un enjeu de sécurité majeur et un enjeu de souveraineté.

Pour une gouvernance internationalisée de l'internet :

Au-delà des stratégies européennes, une prise de conscience internationale émerge pour une nouvelle gouvernance internationalisée de l'internet. Alors qu'elle était contrôlée par les États-Unis depuis 1998, l'organisation en charge des noms de domaines et de la structure technique de l'internet s'ouvre. Une révolution assez discrète pour le grand public, mais dont la portée symbolique est réelle. Depuis le 30 septembre 2016, l'ICANN n'est plus sous la coupe du ministère américain. Cette organisation est l'autorité de régulation de l'Internet, administre les noms de domaines comme le .fr ou le .com des adresses internet et coordonne les acteurs techniques. Elle assure une gestion logistique du réseau au niveau mondial et devrait se prémunir d'influences étatiques qui étaient jusqu'à présent trop marquées.

L'ICANN se transforme, évoluant peu à peu vers une sorte de « Nations unies de l'internet » : une gouvernance pluripartite, fédérée autour de quatre collèges représentant le secteur privé, les experts techniques, la société civile et les gouvernements

Une transition qui marque toutefois un moment constitutionnel crucial pour la refondation de la gouvernance de l'internet car rappelons-le, une grande partie de nos activités se déroule aujourd'hui sur Internet.

SOUS LE POIDS DES GEANTS DU NUMERIQUE : GAFAM, BATX, NATU

Introduction

Les empires de la technologie inquiètent, les GAFAM (Google, Amazon, Facebook, Apple, Microsoft) et autres NATU (Netflix, Airbnb, Tesla, et Uber) transforme nos données des utilisateurs en de nouvelles richesses.

Leur avance prise dans le domaine de la collecte et du traitement des données personnelles, nouvel actif clé du siècle leur permet d'être beaucoup plus performant soutenus par le machine learning et le deep learning pour alimenter l'essor de cette révolution technologique. Cette richesse représente un vrai pouvoir, pas uniquement économique, mais aussi politique.

Les GAFAM exercent des effets pervers sur les mécanismes de l'économie numériques et ils sont critiqués sur plusieurs conséquences de leurs actions, notamment la concentration des entreprises les copyrights, la fiscalité, et pour des raisons éthiques dans leur activité internationale.

Le constat de la domination des plateformes américaines (GAFAM) et bientôt de leurs concurrentes asiatiques (BATX) s'impose à une Europe qui doit s'interroger sur les conséquences économiques, sociales, environnementales et politique. Il y a un réel danger de concentration des activités du GAFAM et NATU. Parfois qualifiée de « colonisation » du numérique européen, elles représentent des risques importants pour l'économie de l'UE mais aussi pour ses entreprises, ses travailleuses et travailleurs, ses citoyennes et citoyens

Aujourd'hui, intimement imbriquées dans nos vies quotidiennes, ces firmes technologiques nous renvoient à une réflexion sur des enjeux éthiques, sécuritaires pour nos entreprises et politiques associés à la souveraineté numérique. Le développement des plateformes numériques interroge le fonctionnement de la démocratie et la stabilité politique de l'UE et des États membres.

Le point sur les chiffres : Analyse

La valorisation boursière mondiale des GAFAM reflète non seulement leur mainmise sur le secteur mais aussi leur poids financier considérable dans l'économie mondiale.

Les capitalisations boursières d'Apple, Alphabet (Google), Microsoft et Amazon sont comprises entre 354 et 837 milliards d'euros, celles des BATX entre 47,5 et 347 milliards d'euros.

Sur le plan des investissements, le poids des géants numériques est impressionnant avec 46,6 milliards d'euros investis au premier semestre 2018 par les 20 premières entreprises du numérique dans le monde, dont 32,5 milliards par les seuls GAFAM, essentiellement dans le domaine du cloud.

En 2018, Apple, suivi de près par Amazon, ont atteint une valorisation financière dépassant 1000 milliards de dollars, ce qui a frappé le monde financier. Les comparaisons avec les PIB des plus grandes économies mondiales étaient mises en évidence (2600 milliards de dollars pour la France, 1600 milliards de dollars pour la Russie). La sommes des valeurs ajoutées d'un pays est un flux annuel, alors que les actions d'une société représentent un stock.

Facebook compte deux milliards d'utilisateurs actifs, soit bientôt un tiers de la population mondiale, mais aussi un milliard sur WhatsApp et 800 millions sur Instagram.

Point de situation sur les dépendances au GAFAM : Chiffres

Le moteur de recherche de Google, Google Search, possède 94% des parts de marché en France. Le système d'exploitation de la firme, Android, est installé sur 9 appareils mobiles sur 10 (monde). La moitié du commerce électronique aux États-Unis passe par Amazon. Le cloud d'Amazon représente 30 % du marché des données dans le cloud.

Le marché mondial des systèmes d'exploitation sur téléphones portables se répartissait en 2018 entre Android (85 %) et IOS (14,9 %), celui sur tablettes à 66 % pour Android, 22,4 % pour IOS et un peu plus de 11 % pour Windows (Microsoft)

Dans le cas des moteurs de recherche, Chrome (Google) captait en août 2018 plus de 67 % des pages vues contre 11 % pour Firefox et 7 % pour Internet explorer (Microsoft), le reste se répartissant notamment entre Safari (un peu plus de 5 %) et Opéra. Google concentre à lui seul 90 % des requêtes sur internet dans le monde.

La position dominante de Google est assez simple à constater puisque Google occupe 91 % des parts de marché sur les 31 États membres de l'Espace économique européen (EEE).

Les GAFAM bénéficient de quasi monopoles de nombreuses propriétés industrielles et intellectuelles, qui sont renforcées par les accords de libre-échange. Elles perçoivent des rentes grâce à la protection des brevets et de leur marque qui reste une source de revenues importantes.

Les dépendances (médias, startups, publicités, innovations, …)

La puissance des GAFAM étant considérable, aujourd'hui elles posent la question du respect des règles de la concurrence.

Ils sont les principaux vendeurs de publicité dans le monde, ce qui leur donne une capacité de financement considérable. Google dispose d'une situation de quasi-monopole dans le domaine des moteurs de recherche, le chiffre d'affaires de Facebook lui par exemple est constitué à 97 % par la vente de messages publicitaires ciblés.

Le marché des moteurs de recherche leur permet de contrôler le référencement des sites et nuit à la transparence des algorithmes déterminant l'ordre d'apparition des résultats de recherche, avec des conséquences lourdes sur l'accessibilité des sites référencés et leur potentiel commercial vis-à-vis des clients.

Les Petites et moyennes entreprises (PME) sont particulièrement vulnérables à ces pratiques du fait de leur taux de recours aux plateformes de services en ligne, qui atteint selon la Commission européenne 42 %, une grande majorité recourant aux moteurs de recherche pour promouvoir ses produits.

Des tests effectués récemment dans six pays par Facebook ont montré comment un ajustement de l'algorithme pouvait priver des sites d'informations des trois quarts de leur trafic. Le résultat démontre comment Facebook, meilleur moteur de ciblage, et Google, meilleur moteur de recherche, ont pris le contrôle de la distribution des créateurs et des médias d'information.

La presse s'inquiète donc de l'utilisation par les GAFAM des informations publiées dans leurs journaux. Il s'agit pour eux d'une appropriation injustifiée de la diffusion des œuvres, des analyses et informations journalistiques sans contreparties. Les créateurs subissent une dépossession d'une partie de leur lectorat, ce qui fragilise leur propre situation économique.

« La presse écrite est en grande difficulté. En France, les recettes publicitaires sont passé de 4 milliards d'euros, à seulement 1,7 milliards d'euros en 2017, alors que Google et Facebook cumulent deux tiers des investissements publicitaires en France ».[58]

Le partage du marché des systèmes d'exploitation sur smartphones entre les seuls opérateurs Google et Apple conduit à ce que l'ensemble des utilisatrices et utilisateurs dans l'UE soient aujourd'hui dépendant d'Android ou IOS pour installer des applications sur leur téléphone. Ces entreprises développant ces applications sont aussi dépendantes des deux géants pour rendre leurs produits accessibles, ce défaut de concurrence est susceptible de nuire à l'économie de notre pays, à la juste fixation des prix, à la qualité des produits ainsi qu'à l'innovation et aux conditions de travail.

Désormais en position de force au vu de leur capitalisation boursière hors norme, ils rachètent des sociétés et empêchent l'arrivée de nouveaux entrants. Grâce à leur puissance financière, qui leur permet de racheter toutes les « startups » susceptibles de produire de nouveaux services technologiquement et économiquement performants, ces monstres américains s'offrent ainsi un temps d'avance sur la concurrence et imposent leurs normes et leur contrôle sur l'ensemble des produits, services et logiciels numériques.

Le pouvoir est beaucoup trop concentré, et il empêche toute rivalité économique et commerciale locale ou régionale. Notre dépendance aux GAFAM constitue un vrai risque technologique, ces entreprises sont un obstacle à nos entreprises, notre résilience économique collective et constitue un risque d'affaiblissement de notre économie ainsi qu'à notre souveraineté numérique.

Les GAFAM et la fiscalité

Champions de l'optimisation et des paradis fiscaux, ces géants, pourtant si riches et si rentables, sont accusés de ne pas prendre part au bien commun des sociétés par l'impôt et de ne pas savoir faire face à leurs nouvelles responsabilités sociales.

Les GAFAM réalisent d'importants profits en recrutant des experts de fiscalité qui leur permet de réduire les charges fiscales ou sociales imposées par les États. Ils ont artificiellement situé leurs activités dans les pays avec un faible taux d'imposition et procèdent à faire remonter la quasi-totalité de leurs chiffres d'affaires vers des pays les plus attractifs en termes de fiscalité.

Localiser leurs profits là où ils sont le moins taxés, pose un vrai problème de compétitivité & sécurité économique en Europe privant les États concernés de ressources budgétaires au détriment du progrès social et nourrissant un profond sentiment d'injustice fiscale. En 2017, elle payait moins de 10 % d'impôt sur les sociétés en Europe, contre une moyenne de 23 % pour les petites entreprises, ce qui pose un réel désavantage économique pour nos entreprises.

A titre d'indication, le bénéfice sur une vente à un client français ne sera pas imposé à 33 %, qui est le taux d'impôt sur les sociétés en vigueur en France, mais à 12,5 % si le siège de la société est en Irlande.

[58] http://www.lefigaro.fr/assets/rapport.pdf

Il paraît donc légitime que les entreprises paient leurs impôts à l'endroit où elles créent leur valeur ajoutée. L'administration Washington sert toujours les intérêts de leurs entreprises et considère que les profits des GAFAM doivent être taxés aux États-Unis, il est très probable que Washington envisagera des mesures de « guerres commerciales » dans l'hypothèse d'une fiscalisation européenne des bénéfices des GAFAM.

Sécurité Globale : les enjeux liés à la sécurité économique des États, implicitement de nos entreprises

Autant commercialement que fiscalement, il y a un impact particulièrement fort sur les acteurs économiques de taille modeste en France et en Europe, qui se retrouvent dans une relation de dépendance vis-à-vis des grandes plateformes. Cette dépendance se traduit beaucoup par des conditions commerciales désavantageuses et d'autres types de pratiques contestables, par exemple en matière de référencement : une situation de monopole sur la publicité et le commerce en ligne se cachant derrière le secret des affaires (des boîtes noires opaques).

La collecte de données est devenue à la fois dangereusement intrusive et très rentable. Nous n'aimons pas l'admettre, mais nous sommes sous surveillance de masse. La plupart des données de surveillance d'Internet sont anonymes par nature, mais les GAFAM sont capables de corréler les informations recueillies avec d'autres informations qui nous identifient avec certitude. Il parait légitime de se poser la question de comment les entreprises américaines se sont retrouvées dans une situation de domination total de notre économie numérique ?

Les relations entre les GAFAM et l'administration gouvernementale des États-Unis sont importantes et réelles, souvent secrètes notamment avec la National Security Agency et les institutions de renseignements des États-Unis, comme en ont témoigné les révélations de Snowden. Les informations stratégiques sont souvent transférées vers les Agences de renseignement américain.

Le lobbying des GAFAM

Il est toujours très difficile de déterminer le coût exact du lobbying des GAFAM. Cependant, il existe des estimations intéressantes fournies par les déclarations faites aux institutions américaines

Les GAFAM exercent des actions de lobbying effrénés (estimés à plus de 100 millions de dollars par an[59]) pour ne pas pâtir de l'exercice normal des lois antitrust. En 2017, Google a été le plus grand contributeur de lobbying exercé auprès des parlementaires ou de la Maison Blanche, soit 18 millions$, ce qui constitue la plus grande contribution de ce type depuis plus de deux décennies, toutes catégories réunies, selon le Center for Responsive Politics.

Les firmes ont des activités de plus en plus hybride, avec un élargissement des gammes de production, pour rendre encore plus difficile l'application des lois qui contrôlent les situations de quasi-monopole. C'est pourquoi l'organisation du lobbying est si importante d'un point de vue législatif et judiciaire pour les GAFAM.

[59] https://lexpansion.lexpress.fr/actualite-economique/pour-le-lobbying-les-gafa-sortent-les-dollars_2002572.html

Les réponses européenne et française face aux GAFAM : point de situation & condamnation

La Commission européenne a toujours combattu et a même interdit certaines opérations de concentration. Les GAFA, Google, Amazon, Facebook et Apple, sont bien une concentration et ils sont curieusement tous américains.

Le RGPD, qui bouleverse profondément le paysage de la publicité est une avancée considérable, puisque les GAFAM ne pourront plus opposer la disparité des réglementations des États membres pour ne pas les appliquer.

Après une guerre intense des lobbys pour définir les règles relatives au copyright, le Parlement européen a voté, le 13 septembre 2018, le projet de directive relative à la protection des droits d'auteur face à l'invasion numérique, en vue d'assurer une réelle rémunération des créateurs et des éditeurs dans le monde d'Internet, c'est officiel Bruxelles souhaite légiférer pour mieux contrôler les contenus.

« *L'article 11 de la directive développe un « droit voisin du droit d'auteur » pour les entreprises de presse sur Internet. Lorsque Facebook et Google utilisent tout ou partie d'un article de presse, ils devront payer des droits d'auteur dont le calcul et le montant n'ont pas été précisés. Les hébergeurs seront responsables des violations du droit d'auteur de leurs usagers* ».

« *L'article 13 demande aux sites d'obliger les internautes qui fournissent des informations issues d'un « créateur » d'obtenir l'accord des titulaires des droits d'auteur. Faute d'accord, les plateformes doivent en empêcher la diffusion. Tous les sites permettant aux internautes de poster du texte, de la vidéo ou du son sont concernés* ».

L'UE cherche à réduire le potentiel de concurrence fiscale anarchique entre les États membres, par une taxation efficace et équitable de l'économie numérique, en vue de définir une assiette consolidée pour l'impôt sur les sociétés. Dans le meilleur des cas, les multinationales seraient dans l'obligation de faire qu'une seule déclaration fiscale consolidée sur le territoire de l'UE. Cette solution constitue une solution pour lutter contre le dumping fiscal. Le 9 juin 2019, un accord de principe aurait été obtenu par le G20 pour la création d'une taxe numérique pour les grandes entreprises de technologie.[60]

Les initiatives de l'UE contre les géants américains commencent à prendre forme mais ne sont pas encore efficace pour inspirer la crainte…Bruxelles montre les dents, multiplie les enquêtes et impose de lourdes amendes. Les pénalités infligées par Bruxelles à l'encontre de Google pour abus de position dominante marquent les esprits.

Les condamnations

Apple a été condamné à l'été 2016 à rembourser 13 milliards d'euros à l'Irlande : la Commission européenne a ordonné à Apple le remboursement de plus de 13 milliards d'euros à l'Irlande pour avoir bénéficié de conditions avantageuses dans le pays.

[60] https://www.developpez.com/actu/265037/Le-G20-appelle-a-la-creation-d-une-taxe-numerique-pour-les-grandes-entreprises-de-technologie-comme-Facebook-Google-et-bien-d-autres/

Facebook a pour sa part été condamné dans plusieurs États membres par les autorités de protection des libertés dans le monde informatique en raison de sa politique de traitement des données personnelles, sans pour autant y mettre un terme. En juin 2017, la commission nationale Informatique et Libertés (CNIL) a condamné Facebook en France à 150 000 €, son homologue espagnol à 1 200 000 € d'amende.

En juin 2017 pour avoir favorisé l'utilisation de son interface de commerce en ligne Google Shopping a été condamné à une amende de 2,42 milliards d'euros, et en juillet 2018 à 4,34 milliards d'euros pour avoir mis en œuvre des pratiques illégales concernant les appareils mobiles Android afin de renforcer la position dominante du moteur de recherche de Google.

Le 21 janvier 2019, suite à la plainte collective déposée par l'association « La Quadrature du Net », la CNIL a prononcé une amende de 50 millions d'euros contre Google en s'appuyant sur le RGPD[61]. En mars 2019, conformément à l'article 102 du traité sur le fonctionnement de l'UE, la Commission européenne a infligé une troisième amende de 1,49 milliard d'euros à Google, l'accusant, une fois de plus, d'abuser de sa position dominante au détriment de la concurrence « des pratiques illégales de courtage en publicité par les agences de recherche afin de renforcer sa position dominante sur le marché ». Cette fois, une obligation de mettre fin à ses pratiques anticoncurrentielles a été mis à l'évidence sous peine d'une nouvelle sanction plus forte.

Conclusion : trop grands, trop puissants, trop négligents, trop longtemps

L'Union européenne s'est résignée à l'hégémonie américaine, elle n'a jamais pris le parti, à l'image de la Chine avec Alibaba ou la Russie avec Yandex, d'accompagner l'essor d'un champion national capable de lutter à armes égales avec Google ou Amazon.

La question des monopoles est une vraie question, lorsqu'une économie a tendance à se retrouver sclérosée par quelques monopoles qui assurent à eux seuls de multiples secteurs d'activité et couvrent une grande part des capitaux financiers disponibles au détriment de la dynamique économique, le problème de ces monopoles… c'est que l'économie politique à l'œuvre commence à se voir un peu trop. Résister à la colonisation du web par les GAFAM devient un vrai sujet de sécurité économique de nos entreprises.

Malgré les efforts en cours de la part de la Commission européenne, les géants du Web accumulent aujourd'hui des données qui mettent en danger notre économie et la protection de nos entreprises.

Comme vu précédemment, les GAFAM sont sources d'inégalités et de division de la société, siphonage des revenus des créateurs et des médias avec prise de contrôle. Il convient dès lors de développer des infrastructures alternatives -compatibles, peut-être, mais indépendantes des systèmes actuels, développer une culture de la pluralité des systèmes et de prendre les mesures permettant de favoriser l'hétérogénéité du monde numérique, encourager l'open source et les systèmes décentralisés.

[61] http://europa.eu/rapid/press-release_IP-19-1770_fr.htm

Ces géants technologies ont trop de pouvoir, trop de pouvoir sur notre économie, notre société et notre démocratie. Elles ont écrasé la concurrence, utilisé nos enseignements personnels à des fins lucratives et faussé les règles du jeu contre tout le monde. Ce faisant, elles ont nui aux petites et moyennes entreprises et étouffé l'innovation.

Le fait que l'UE ne soit pas parvenue à ce jour à faire naître un géant du numérique capable de rivaliser avec les grandes plateformes américaines, voire asiatiques, a conduit celle-ci à promouvoir un modèle spécifique de société numérique autour de valeurs (protection des données personnelles, concurrence loyale, fiscalité équitable, autorité des régulations…) dont la dimension défensive pourrait parfois être perçue comme une forme d'antiaméricanisme.

LES INVESTISSEMENTS STRATEGIQUES : LES FONDS VAUTOURS

S'il y a un bien un phénomène qui s'est fait connaître au cours des années 2000, et qui est redoutable, c'est celui des fonds vautours ou *vulture fund* ou parfois *activist investors* en anglais.

Il s'agit là de fonds d'investissements dont la cible est le rachat à bas prix de dette d'entreprises et dont l'objectif final est de réaliser une plus-value « soit par la restructuration de la dette soit en refusant la restructuration et en obtenant par action en justice le remboursement de leur créance à une valeur proche de la valeur nominale plus intérêts ».

Les cibles de ces fonds sont par exemple des entreprises en très grandes difficultés proches du défaut de paiement. En pareil cas, les titres sont très dépréciés, les investisseurs « normaux » les ayant cédés par crainte de non-remboursement de la dette. Toute la stratégie des fonds vautours va consister à évaluer ce qu'ils pourront retirer de ces titres si l'entreprise disparaît. En pareil cas, les créanciers de l'entreprise rentrent rarement dans leurs frais, mais peuvent parfois toucher un certain pourcentage de leurs créances sur l'entreprise défaillante, grâce à la vente des actifs de cette dernière. Comme un fonds vautour aura acheté des titres lui donnant droit à une créance sur l'entreprise, mais à un prix très inférieur à la valeur nominale, il peut espérer une plus-value. Celle-ci sera souvent obtenue par décision d'un tribunal administratif, ce qui fait que l'activité des fonds vautours est assez différente des activités d'investissement traditionnelles, où l'on mise plutôt sur la réussite d'une entreprise que sur sa perte. On a notamment vu les fonds vautours à l'œuvre dans l'affaire Madoff, lors de laquelle ils ont racheté des parts de fonds vendus par le célèbre escroc en essayant ensuite d'obtenir réparation[62]

Pour comprendre le concept : les taux de recouvrement représentent en moyenne 3 à 20 fois leur investissement, ce qui équivaut à des rendements de 300 % à 2 000 %.[63]

Stratégies offensives, quand l'État est la cible

Ces fonds représentent une véritable menace dans l'écosystème financier, il perturbe la stabilité des entreprises et des états. Leurs actions offensives peuvent déstabiliser des

[62] https://www.challenges.fr/tag_lexique-economique/fonds-vautours_5357/
[63] https://gestion-de-patrimoine.ooreka.fr/astuce/voir/581575/fonds-vautour

gouvernements, dans leurs politiques, leurs développements et tout ce qu'il en découlerait par des « phénomènes de réaction en chaîne ».

Exemple : un fonds vautour a racheté une dette de 3 milliards de dollars, a poursuivi la Zambie pour 55 millions de dollars et s'est vu attribuer 15,5 millions de dollars.

Au moins 20 pays d'Afrique ont été menacés ou ont fait l'objet d'actions en justice de la part de fonds vautours :

- La Sierra Leone par Greganti Secondo et Arcade.
- La Côte d'Ivoire et le Burkina Faso par Industrie Biscoti.
- D'autres PMR ont été visés : l'Angola, le Cameroun, le Congo, la République démocratique du Congo, l'Éthiopie, le Liberia, Madagascar, le Mozambique.

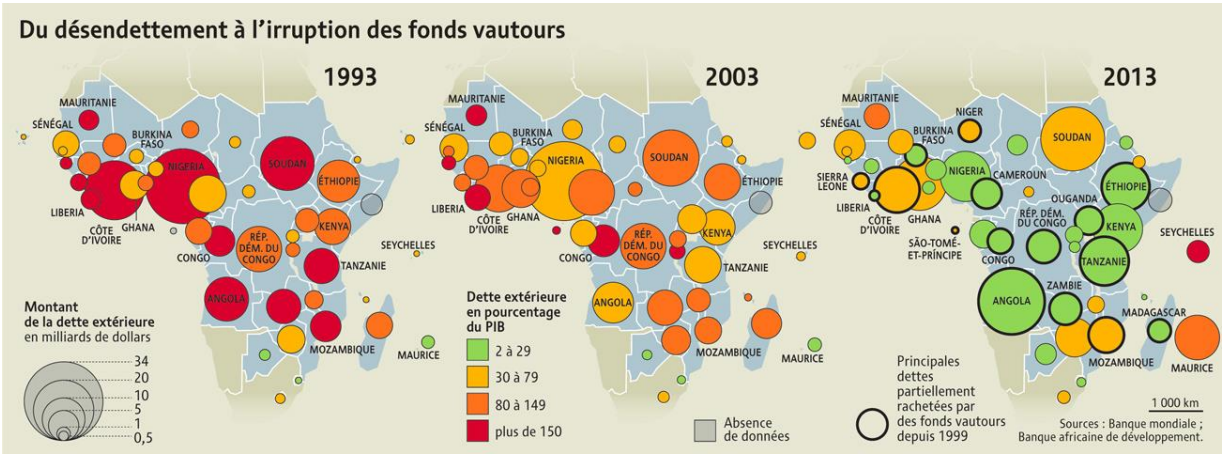


Figure 14 : Exemple de Stratégie fond vautour[64]

Actuellement, 11 pays seraient la cible de 44 procès intentés par des créanciers privés - pour l'essentiel des fonds vautours - qui réclament 1,9 milliard de dollars au total, d'après le Fonds monétaire international (FMI).

Les plus grosses sommes sont demandées à la République du Congo (900 millions de dollars de dédommagements déclarés), au Cameroun (347 millions de dollars) et au Nicaragua (276 millions de dollars).[65]

Par quels mécanismes les fonds vautours ont-ils cherchés à exploiter les opportunités de la faillite Grec ?

Un autre cas d'école aujourd'hui à citer en exemple serait celui de la Grèce depuis le début de la crise au sein de la zone Euro. Au regard de sa dette et de son déficit croissant, Athènes s'est retrouvé en défaut de paiement faute d'avoir pu rembourser ses créances au FMI. Des fonds activistes, dit fonds vautours ont donc commencés à étudier les opportunités de la faillite Grec. Le taux d'endettement du pays est d'environ 172% du PIB en 2011. Les fonds vautours vont alors s'engager dans le rachat massif de dette Grec. Peu de temps après, un inévitable processus de restructuration de la dette est mis en marche. Ces fonds vont alors réaliser une

[64] https://www.monde-diplomatique.fr/cartes/dette-vautours-afrique
[65] http://www.patrimoinorama.com/index.php?option=com_content&task=view&id=4039&Itemid=29

forte plus-value car les titres qu'ils ont obtenu grâce à la restructuration donnaient droit à des remboursements supérieurs au prix d'achat. Une grande majorité de ces fonds vont cibler spécifiquement les titres de la dette grecque soumis au droit étranger (majoritairement le droit anglais) dans leurs rachats. On estime aujourd'hui ce total à 6,4 milliards détenus par des fonds vautours.

Le cas Vivendi-Telecom Italia

Depuis Juin 2017, le plus célèbre *activist fund* américain (à la réputation de fond vautour), Elliott Management, est monté au capital de ces sociétés et a racheté des titres.

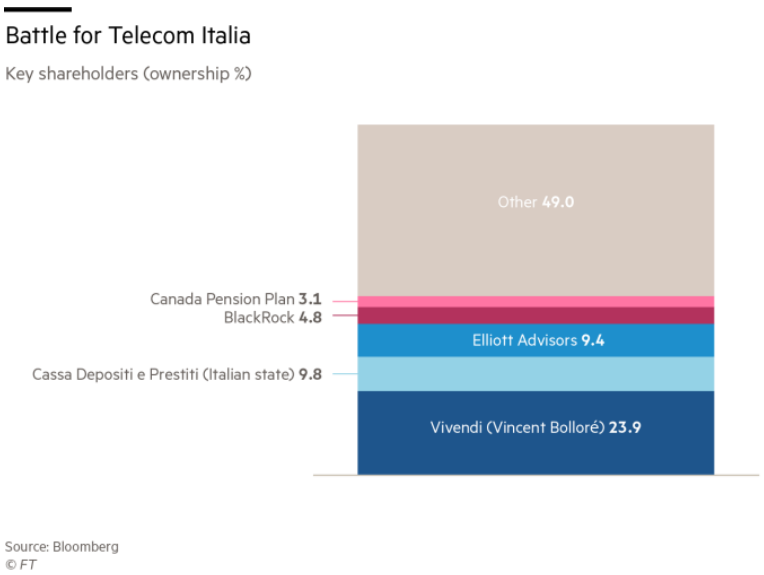


Figure 15 : Combat pour Telecom Italia

Elliott Management possède à ce jour plus de 9% des actions TIM ce qui lui permet de contrôler la gestion de l'actionnaire majoritaire. « En Mai 2018, Elliott renverse le conseil d'administration où Vivendi, actionnaire de référence, avait la main. Dans la foulée, le conseil renvoie le PDG, un proche de Vincent Bolloré. [66] » Selon un récent article paru dans Bloomberg, les fonds vautours américains sont en phase d'OPA du marché des télécoms et médias européens. On peut ainsi lire une stratégie offensive de contrôle sectorielle. Ils ont ainsi un contrôle sur la gouvernance de l'entreprise et pourrait tout aussi bien s'en servir pour jouer de stratégie afin d'affaiblir ces groupes et donner ainsi l'avantage à d'autres entreprises américaines dans secteurs concurrentiels au sein desquelles ils ont des intérêts.

« Le système économique n'a pas été corrigé depuis 2008. La financiarisation est toujours là. Le plus grave est la cécité de certaines entreprises pour prendre en compte les enjeux de long terme. »

A très court terme, les économistes s'accordent à dire que nous allons observer des vagues de fusions-acquisitions et ce, en partie à cause à la réforme fiscale de Trump qui est considéré comme un outil de conquête de nos entreprises.

[66] https://lexpansion.lexpress.fr/actualite-economique/paul-elliott-singer-le-financier-qui-fait-trembler-l-europe_2058821.html

CONCLUSION

Il est indéniable que la sûreté-sécurité des entreprises a fait des progrès importants ces dernières années. Les grands groupes ont désormais une direction dédiée avec des moyens humains et financiers pour faire face aux enjeux de sûreté-sécurité. Au-delà de la sécurité classique, certaines entreprises ont pris en compte l'intelligence économique et le cyber espace dans leur stratégie de protection et ont décloisonné ces domaines pour gagner en efficacité. Néanmoins, l'accélération des risques et des vulnérabilités, notamment dans le domaine immatériel, oblige les entreprises à mettre en place toujours plus de moyen pour se protéger. Elles ont encore des difficultés à s'organiser pour anticiper et se prémunir de tous ces risques. Une solution passe par la mitigation de ces risques par les assurances mais également par des capacités de résilience pour faire face aux crises rencontrées en mettant en place des moyens de gestion de crise et de continuité d'activité.

Face aux menaces que représente le patriotisme économique de pays comme les États-Unis ou la Chine, les grands groupes n'ont pas les moyens d'être autonome dans leur défense. En effet, des armes de guerre économique comme l'extraterritorialité du droit américain ou les dépendances sont redoutables pour l'entreprise mondialisée. Même avec l'appui de leur État, ces dernières restent vulnérables à l'image de Huawei, mais également celles qui en dépendent et sont des victimes collatérales de ces affrontements. Les menaces des sanctions américaines suffisent à freiner les ambitions de développement économique des entreprises, notamment pour les entreprises européennes, mal protégées ou peu soutenues par leur État.

Actuellement, les pays européens comme la France, cherchent encore des réponses pour faire face aux rapports de force économiques des États-Unis et de la Chine. Ces États affaiblissent leurs entreprises et qui rendent leur économie de plus en plus dépendantes, notamment dans le monde immatériel.

L'entreprise ne peut pas se défendre toute seule sans l'aide d'un État fort avec une stratégie de puissance. Même si des grands groupes se protègent mieux que d'autres, le concept de sécurité globale est utopique pour les entreprises et en particulier leur sécurité économique.

BIBLIOGRAPHIE

- Ali Laïdi, « Le Droit, nouvelle arme de guerre économique » aux éditions Actes Sud, 2019
- Frédéric Pierruci, « Le piège Américain » aux éditions JC Lattès, 2019
- INHESJ, « Maîtrise des risques et des crises : une réflexion croisée » GT3P, 2008
- « Le management des risques de l'entreprise » (IFACI et PriceWaterhouse Coopers Landwell, 2005)
- Question Sécu, Jérôme Saiz, mai 2019, « Vers une sécurité globale : sécurité économique, sûreté et cybersécurité », https://questionsecu.fr/vers-une-securite-globale-securite-economique-surete-et-cybersecurite/
- France Culture : « Guerre économique : comment les Etats-Unis font la loi », https://www.franceculture.fr/economie/guerre-economique-comment-les-etats-unis-font-la-loi
- France Culture : « Vers une nouvelle guerre froide économique ? », https://www.franceculture.fr/emissions/la-grande-table-2eme-partie/vers-une-nouvelle-guerre-froide-economique
- Journal de l'économie, Olivier de Maison Rouge : « Les conséquences juridiques du « Cloud act » US en matière de collecte des données », https://www.journaldeleconomie.fr/Les-consequences-juridiques-du-%E2%80%89Cloud-Act%E2%80%89-US-en-matiere-de-collecte-internationale-des-donnees_a7352.html
- Bernard Cazeneuve, interview ICDM mai 2019 « L'extraterritorialité du droit US en action », https://youtu.be/abqHnseJxXM
- Colloque annuel 2018 du CDSE : « La sécurité au cœur du Business »
- Conférence SYNFIE juin 2019 : « Diplomatie économique et sécurité des entreprises »
- Conférence AEGE février 2018, Olivier Hassid (PwC) : « La transformation de la fonction Sûreté : vers un nouveau paradigme »
- https://www.diplomatie.gouv.fr/IMG/pdf/PSD_266_Dossier_Reforme.pdf
- https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/legislative/2003_combat_terr.pdf Page 6
- https://www.dhs.gov/sites/default/files/publications/DHS BIB 2019.pdf
- https://www.dhs.gov/about-dhs
- http://www.assemblee-nationale.fr/12/pdf/rap-info/i1664.pdf
- http://www.leppm.enap.ca/leppm/docs/Rapports_securite/Rapport10_sécurité.pdf
- https://www.sipri.org/research/conflict-and-peace/asia/china-and-global-security
- https://www.letemps.ch/monde/guoanbu-puissance-renseignement-chinois
- https://nationalinterest.org/feature/dangerous-love-chinas-all-encompassing-security-vision-16239
- https://www.lesechos.fr/industrie-services/air-defense/surete-les-fusions-acquisitions-en-pleine-effervescence du 11/04/2019

- https://www.lesechos.fr/finance-marches/ma/nouvelle-alliance-dans-la-surete du 13/06/2019
- https://www.ege.fr/download/metiersIE_AEGE2019.pdf
- F-Secure, Le trafic des cyberattaques, 5 Mars 2019
- Baromètre cybersécurité 2019 Sylob, Usine Nouvelle et Hub One, 21 Février 2019
- Quelles sont les différents types de cybercriminalité, Panda Security, 23 Janvier 2019
- Une analyse économique du piratage informatique, Revue de Sciences humaines, Peter T. Leeson, 1er Janvier 2017
- Commission d'enquête sur la souveraineté numérique, 23 Mai 2019
- https://portail-ie.fr/resource/glossary/44/securite-economique
- https://portail-ie.fr/short/2042/les-zones-dombre-de-laffaire-alstom-selon-frederic-pierucci
- http://www.fcpablog.com
- /blog/2019/3/11/with-mts-in-the-new-top-ten-just-one-us-company-remains.html
- http://www.fcpablog.com/
- https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
- http://www.lefigaro.fr/secteur/high-tech/outre-huawei-quels-sont-les-groupes-chinois-sur-la-liste-noire-de-donald-trump
- https://www.numerama.com/donald-trump-exclut-huawei-des-telecoms-aux-usa-au-nom-de-lurgence-nationale.html
- https://www.reuters.com/article/us-huawei-tech-usa-facebook/facebook-suspends-app-pre-installs-on-huawei-phones
- https://www.lerevenu.com/bourse/huawei-dans-la-tourmente-soitec-et-stmicro-trinquent-en-bourse-nokia-en-profite
- https://fr.reuters.com/article/frEuroRpt/idFRL5N22W11U
- https://www.soitec.com/media/upload/1_assemblee_generale/20180726_AGOE_VF/Soitec-DDR-2017-2018-VFfinale.pdf
- https://fr.reuters.com/article/businessNews/idFRKCN1TE36A-OFRBS
- https://www.tomsguide.fr/huawei-la-liste-des-deserteurs-sallonge/
- https://www.mesactions.com/economie-et-finances/les-groupes-americains-aussi-font-les-frais-des-sanctions-contre-huawei
- https://fingfx.thomsonreuters.com/gfx/editorcharts/USA-CHINA-HUAWEI/0H001GSE93H2/index.html
- https://www.ledevoir.com/economie/555786/guerre-commerciale-la-chine-sort-une-liste-noire-d-entreprises-non-fiables
- https://www.zdnet.fr/actualites/les-consommateurs-chinois-ont-boude-l-iphone-et-d-autres-smartphones-39879847.htm
- https://www.bloomberg.com/news/articles/2019-05-22/apple-earnings-could-be-slashed-29-on-a-china-ban-goldman-says
- https://www.phonandroid.com/huawei-lexclusion-du-constructeur-va-faire-des-degats-enormes-estime-arm.html
- https://www.magazine-decideurs.com/classements/compliance-programmes-de-conformite-classement-2018-cabinet-d-avocats-france-1
- https://infoguerre.fr/2019/04/guerre-economique-question-essentielle-encerclements-cognitifs/
- http://www.lefigaro.fr/assets/rapport.pdf

- https://lexpansion.lexpress.fr/actualite-economique/pour-le-lobbying-les-gafa-sortent-les-dollars_2002572.html
- https://www.developpez.com/actu/265037/Le-G20-appelle-a-la-creation-d-une-taxe-numerique-pour-les-grandes-entreprises-de-technologie-comme-Facebook-Google-et-bien-d-autres/
- http://europa.eu/rapid/press-release_IP-19-1770_fr.htm
- https://www.challenges.fr/tag_lexique-economique/fonds-vautours_5357/
- https://gestion-de-patrimoine.ooreka.fr/astuce/voir/581575/fonds-vautour
- https://www.monde-diplomatique.fr/cartes/dette-vautours-afrique
- http://www.patrimoinorama.com/index.php?option=com_content&task=view&id=4039&Itemid=29
- https://lexpansion.lexpress.fr/actualite-economique/paul-elliott-singer-le-financier-qui-fait-trembler-l-europe_2058821.html