Guerre de l'information

« Guide de survie pour entreprise »

Comment se défendre et passer à l'attaque légalement dans la jungle informationnelle et concurrentielle à laquelle doit désormais faire face toute entreprise ?

Anne-Sophie Toumi

Franck Lambaudie

Xavier Paque

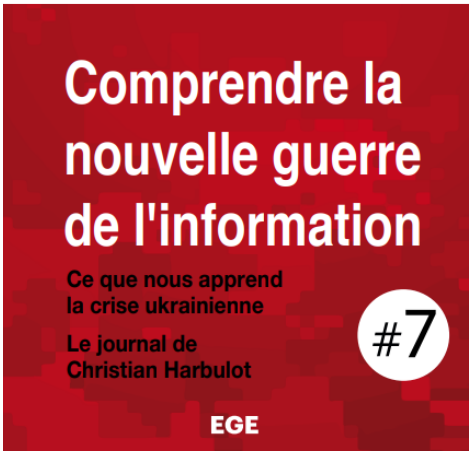
Anthony Suarez

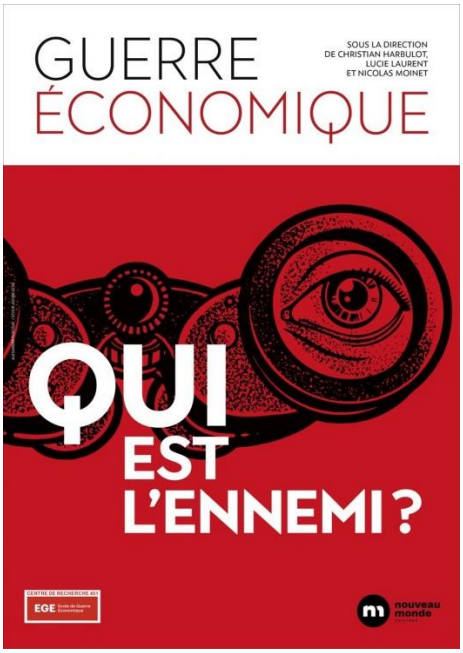
Edouard Jeulin

EGE Ecole de Guerre Economique

Table des matières

CAHIERS
DE LA
GUERRE ECONOMIQUE





Introduction

Depuis son apparition sur Terre, l'Homme n'a pas cessé d'innover dans le but de faciliter, d'améliorer ses tâches quotidiennes. Il est donc aisé de dire que le progrès a toujours fait partie intégrante de l'histoire de l'humanité. Toutefois, les évolutions se sont étalées sur le temps long de l'Histoire. Néanmoins, la période contemporaine marque une rupture nette avec le « rythme de croisière » du progrès. La révolution de l'informatique, de l'Internet et des Nouvelles Technologies de l'Information et de la Communication (NTIC) a littéralement fait entrer l'humanité dans une nouvelle dynamique. Cette nouvelle ère est caractérisée par une forte accélération du rythme du progrès. La mesure de leurs impacts sur nos modes de vie, nos modes de consommation, notre manière de faire de la politique et même de penser sont incommensurables. Les lignes sont désormais mouvantes. Les évolutions technologiques bouleversent notre monde, notre quotidien et surtout les codes et règles qui régissent les interactions sociales, notre système politique comme notre façon de nous informer face à la masse d'informations disponibles en sources ouvertes. La dimension et l'emprise stratégique de ces NTIC est telle que l'on parle depuis le début des années 2000 de «société de l'information». Cette dernière a été définie en 2001 par Eskanen-Sundström comme « une société qui fait un usage intensif des réseaux d'information et de la technologie de l'information, produit de grandes qualités de biens et de services d'information et de communication et possède une industrie de contenus diversifiée »[1].

Ces évolutions technologiques se sont matérialisées par une écrasante inflation d'informations disponibles en sources ouvertes. Ce faisant, le spectre de l'intelligence économique (IE) a été élargi. En effet, en France, les premiers travaux sur l'intelligence économique ont été réalisés avant l'avènement de l'Internet et de la société de l'information, entre 1992 et 1993. Ils ont abouti au Rapport Martre, intitulé « Intelligence économique et stratégie des entreprises ». Le but du rapport était alors de comprendre les nouveaux cadres de la concurrence et de la compétitivité dans le monde post-guerre froide. L'intelligence économique est alors définie « comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques »[2]. Cela était mené légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise »[3]. Par information utile, il est fait référence à celle dont ont besoin les différents niveaux de décision de l'entreprise ou de la collectivité, pour élaborer et mettre en œuvre de façon cohérente la stratégie et les tactiques nécessaires à l'atteinte des objectifs définis par l'entreprise dans le but d'améliorer sa position dans son environnement concurrentiel[4]. Le but d'une telle démarche est alors de générer « une vision partagée des objectifs à atteindre »[5]. Quelques années plus tard, les apports du rapport Martre à l'intelligence économique française ont été complétés avec l'aspect guerre de l'information.

L'entrée dans l'ère de l'immédiateté et des réseaux sociaux, génère l'émergence de nouvelles menaces auxquelles l'ensemble des acteurs de la société sont ou vont être confrontés. Au premier chef de ces derniers, se trouvent les États. Les États démocratiques occidentaux y sont d'ailleurs extrêmement sensibles et ce pour plusieurs raisons. Après la chute du mur de Berlin et la fin de la Guerre Froide, la « fin de l'histoire » a été actée par des théoriciens, estimant que le monde entrait alors dans une ère de paix et de prospérité grâce à l'économie. Autrement dit, la pensée dominante voulait alors que la mondialisation, les échanges commerciaux tarissent les tensions géopolitiques, les ambitions

[1] **BALIMA Serge Théophile.** « Une ou des « sociétés de l'information » ? », *Hermès, La Revue*, 2004/3 (n° 40), p. 205-209. DOI : 10.4267/2042/9540. [En ligne] **https://www.cairn.info/revue-hermes-la-revue-2004-3-page-205.htm** [Consulté le 21 avril 2022]

[2] **MARTRE, Henri. 1994.** *Intelligence économique et stratégie des entreprises*. Paris : La Documentation Française. Premier rapport étatique comportant le terme intelligence économique dans son titre. Page 11

[3] **Idem**

[4] **Ibid**

[5] **Ibidem**

stratégiques et les enjeux de puissance. Ce fourvoiement a été particulièrement marqué en Europe et s'est matérialisé par une certaine naïveté visible à bien des égards (économique, stratégique, géopolitique). Néanmoins, ces dernières années ont été marquées par une série de crises qui ont sonné aux oreilles européennes comme un début de prise de conscience. Les dépendances stratégiques européennes ont été mises en exergue par la pandémie de Covid-19 tandis que le retour de la guerre sur le continent européen, avec le déclenchement de la guerre en Ukraine, a fini de démontrer que la « fin de l'histoire » n'était qu'un mythe, une utopie. Il suffisait pourtant de regarder en dehors du territoire européen où les guerres et le « grand jeu » des puissances internationales n'ont pas cessé ces trente dernières années.

Alors que l'on passe d'un monde unipolaire, marqué par la puissance américaine, à un monde multipolaire, où les « États carnivores »[6] en plein essor - Russie, Chine, Turquie - veulent également affirmer leurs positions et leurs ambitions, la question de la puissance est bien au centre de l'échiquier. Toutefois, les modalités de puissance évoluent également. Désormais, l'aspect des nouvelles technologies et son corollaire de guerre informationnelle ou encore de « soft power » sont prépondérants dans les stratégies de puissance des États.

Dans une logique de clarté, nous reprendrons la définition de «la guerre de l'information [GI] ou infoguerre, comme une combinaison d'actions humaines ou technologiques destinées à l'appropriation, la destruction ou la modification de l'information. Elle se décline en trois logiques, par, pour et contre : manipulation de la connaissance, maîtrise des canaux de diffusion et interdiction d'émission »[6].

Par ailleurs, à la GI par le « contenu » (textes et narratifs nourrissant la GI), s'ajoute également celle du « contenant » (la cybersécurité et ses outils).

C'est par ces deux aspects que nous avons choisi d'aborder la GI.

Dans ce contexte de réveil brutal, la guerre informationnelle est au cœur des enjeux de la survie des États démocratiques. De fait, les « États carnivores »[7] tentent de saper et d'affaiblir les fondements de ces sociétés, par des campagnes de manipulation de l'information notamment, en jouant sur leurs propres contradictions. C'est dans ce contexte que ces États s'arment, à l'instar de la France avec la création de VIGINUM à l'été 2021, entité chargée de lutter contre les manipulations de l'information étrangères visant la France, pour contrer le phénomène.

Si les États sont clairement au centre de cette guerre informationnelle, les opérateurs économiques privés ne sont pas en reste. La scène économique, très concurrentielle, est également aux prises avec ces problématiques. Les arnaques aux présidents, les allégations mensongères destinées à « casser » le concurrent, ou autres attaques informationnelles sont des réalités auxquelles les dirigeants de PME/ETI sont peu sensibilisés et surtout peu armés pour y faire face. Au-delà du fait que nombre de ces dirigeants ont peu de temps à consacrer à ces problématiques, qui sont pourtant primordiales pour la survie de leur entreprise, il semble également que la littérature disponible sur le sujet soit très théorique et insuffisamment lisible et pragmatique pour les entreprises. Il nous apparaît donc que ce manque « d'opérationnalité » freine certaines entreprises à mettre en place leur stratégie.

[6] **Centre de ressources et d'information sur l'intelligence économique et stratégique.** Guerre de l'information. *Portail de l'IE.* [En ligne] [Consulté le : 25 mars 2022.] https://portail-ie.fr/resource/glossary/97/guerre-de-linformation

[7] Expression employée par la Central Intelligence Agency (CIA) dans son rapport prospectif de 2021 sur « le monde en 2040 » (National Intelligence Council, Le monde en 2040, Editions des Equateurs, 2021, 256p). Les États carnivores sont définis comme étant des États privilégiant la « force brute et la politique du fait accompli » face à la paralysie des instances multilatérales.

Comment une entreprise peut-elle mettre en place une stratégie de protection face à la guerre de l'information afin de pérenniser son développement voire assurer sa survie en tenant compte de ses contraintes et de son exposition au risque ?

Pour parvenir à la définition d'une stratégie pérenne, l'entreprise doit baser son analyse sur un outil agile articulé autour de ses contraintes, sa maturité, et l'évolution de son exposition aux risques. Nous proposons de fournir un outil d'évaluation dont le résultat permet une priorisation des actions à mener sur les sujets de guerre de l'information.

Pour ce faire, nous articulons notre raisonnement autour de quatre grands axes. Dans un premier temps, nous en nous appuyant sur le référentiel MITRE ATT&CK, nous établirons une revue de littérature nous permettant de traiter tant le contexte de la guerre de l'information que les outils à disposition pour y faire face. Dans un second temps, nous exposerons l'enquête empirique que nous avons menée avant, dans un troisième et dernier temps, de présenter notre modèle d'évaluation.

Pour ce faire, nous appuyons notre démonstration sur quatre principales parties :

1. Dans un premier temps, nous proposons de dresser un panorama global du contexte et des enjeux propres à la guerre informationnelle.
2. Fort des constats posés dans cette première partie, nous proposerons de rapprocher les notions de cybersécurité et d'intelligence économique au travers du référentiel unique pour émettre nos préconisations sur une base commune.
3. Ensuite, nous détaillerons l'ensemble des outils à mettre en place pour les entreprises dans notre guide de survie. Ces outils rassembleront aussi bien les aspects défensifs qu'offensifs à disposition dans les limites du cadre légal.
4. Nous conclurons enfin sur la proposition d'une grille d'évaluation complète qui permettra aux entreprises d'évaluer leurs forces et leurs faiblesses, et ainsi prioriser leurs actions parmi celles proposées en partie N° 3 de ce plan.

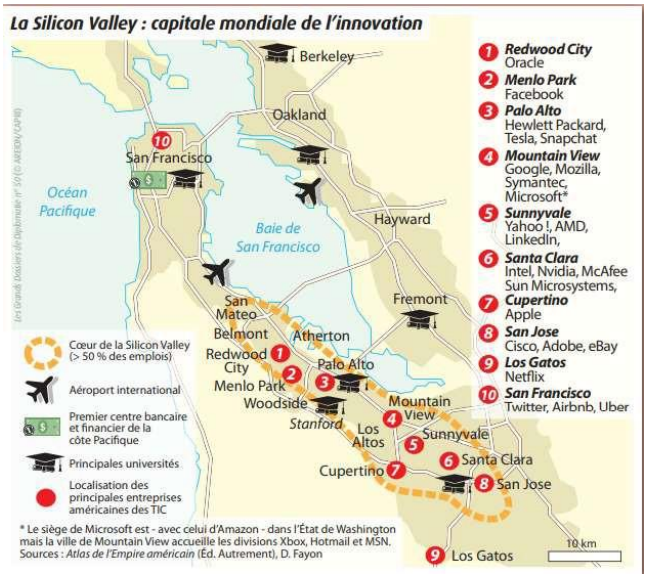
Chapitre 1

Guerre de l'information : qu'entend-on par cette expression ?

1.1. Révolution technologique : passage à l'ère du numérique et de l'information

L'essor de la société de l'immatériel a fait de l'information un outil hautement stratégique dont l'usage peut aussi bien être défensif, offensif ou encore un vecteur d'amélioration. Le caractère stratégique que revêt désormais l'information est l'aboutissement de plusieurs décennies de bouleversements technologiques dans les domaines des communications et des réseaux de transmission notamment. Le développement fulgurant des Nouvelles Technologies de l'Information et de la Communication (NTIC) a propulsé le monde dans l'âge de l'Internet et de l'information et suscité une véritable révolution numérique au sein de nos sociétés. Cela a naturellement fait évoluer nos façons de nous comporter, de nous informer, de socialiser ou encore de faire de la politique. A titre d'illustration, il suffit de jauger l'espace et l'influence de plus en plus marqués qu'occupent les réseaux sociaux dans nos sociétés contemporaines. Leur usage se fait à géométrie variable : pour le pire, comme lors de l'assassinat du professeur Samuel Paty en octobre 2020, et le meilleur, comme lors d'élans de solidarité en faveur d'une cause quelconque.

Par ailleurs, ces changements ont généré un point de rupture majeur avec le « monde d'avant ». En effet, le nombre de données disponibles en source ouverte a littéralement explosé. Internet a non seulement permis un partage illimité de l'information mais a ainsi décuplé le nombre d'informations disponibles. Face à cette masse de données en accès libre, de nouvelles questions ont logiquement émergé autour de leur contrôle et de leur interprétation. Cela a, très tôt, suscité des convoitises dans les pays, comme les États-Unis, ayant traditionnellement une forte culture stratégique et une appétence déjà marquée pour la maîtrise et le partage de l'information, considérée comme un « levier de survie »[8]. C'est d'ailleurs l'un des facteurs explicatifs de l'hégémonie américaine dans ce domaine tant du point de vue légal, avec notamment la question de l'extraterritorialité du droit américain[9], que purement technologique avec la puissance des GAFAM (Google, Apple, Facebook, Amazon, Microsoft).



Les grands dossiers de Diplomatie N°50, Affaires stratégiques et Internationales, Les GAFAM sont-ils trop puissants? Entretien avec Julien Nocetti ; Avril - Mai 2019 ; P88-89

[8] **HARBULOT, Christian. 2001.** Les principes de la guerre de l'information. *Infoguerre*. [En ligne] 14 novembre 2001. [Consulté le 25 mars 2022.] https://www.ege.fr/infoguerre/2001/11/les-principes-de-la-guerre-de-l-information.

[9] Pour prendre conscience de la puissance de feu de l'extraterritorialité du droit américain, il faut regarder les affaires BNP Paribas (amende de 7 milliards USD) et Crédit Agricole (amende de 787 millions USD).

Face à cette suprématie américaine, certains pays, conscients des questions stratégiques et de souveraineté qui se cachent derrière la révolution numérique, ont élaboré des stratégies visant à se départir de cette dépendance à la technologie américaine. C'est le cas de la Chine qui a facilité le développement de ses BATXH (Baidu, Alibaba, Tencent, Xiaomi, Huaweï) et a interdit l'utilisation de Google dès 2010. A l'inverse le « Vieux Continent », et en particulier la France, culturellement moins ouvert à l'anticipation stratégique, est à la traîne de la course mondiale à la souveraineté technologique, demeurant in fine très dépendant des technologies américaines. Toutefois, à l'aune des dernières crises mondiales (Covid, Ukraine), un certain réveil désenchanté semble s'opérer tant du côté des entreprises que de la population. Toutefois, il faut engager une véritable « révolution culturelle » afin de changer le management de l'information qui demeure très individuel en France.

L'ensemble des évolutions technologiques a clairement fait entrer le monde dans l'ère de l'information voire même dans « l'ère de la surinformation »[10]. Face à cet amas toujours plus important de données, l'enjeu est désormais d'identifier l'information pertinente, vectrice de plus-value pour l'entreprise.

1.2. Emergence de nouvelles menaces

Dans ce contexte, il est donc aisé d'affirmer qu'au 21ème siècle, l'évolution des rapports de force, des guerres qu'elles soient physiques ou économiques se joue autour de la maîtrise de l'information. Cet état de fait a fait émerger de nouvelles menaces d'ordre informationnel et cyber. La courbe d'évolution de ces menaces est exponentielle. Par ailleurs, elles sont d'autant plus prégnantes que les récents événements géopolitiques et sanitaires ont fortement décrédibilisé la grille de lecture jusqu'alors dominante. En effet, la douce musique de la « mondialisation heureuse », selon laquelle le développement des relations économiques entraînerait la paix et la prospérité à l'échelle mondiale, jugeant ainsi caduc les enjeux de puissance, d'intérêts et de souveraineté, a fortement été affectée par les épreuves successives de la Covid-19 et de la guerre en Ukraine. Les faiblesses de cette grille de lecture ont été mises au jour. A l'inverse, les grilles de lecture relatives à la permanence des enjeux de puissance entre États, à la compétition économique mondiale ont, elles, été validées.

Cet état de la menace informationnelle est désormais largement pris en considération par les autorités françaises. D'ailleurs, la nouvelle vision stratégique du chef d'état-major des armées, Thierry Burkhard, dévoilée en octobre 2021, prend largement en compte ces nouveaux enjeux. Cette doctrine, qui peut d'ailleurs se résumer par l'axiome « gagner la guerre avant la guerre », prend en considération les nouvelles stratégies de puissance des États qui concernent des champs d'action de plus en plus étendus à mesure que « les activités humaines s'étendent à de nouveaux de domaines »[11]. Ces nouveaux domaines sont cités comme étant les milieux exo-atmosphérique, cyber, les grands fonds marins, les champs électromagnétiques et l'informationnel. Cela a comme conséquence logique d'étendre également les espaces de conflictualité. La multiplication des domaines de confrontation favorise la mise en place de « stratégies hybrides et de contournement ». Il s'agit de combiner « des modes d'actions militaires et non militaires, directs et indirects, réguliers ou irréguliers, souvent difficiles à attribuer, mais toujours conçus pour rester sous le seuil estimé de riposte ou de conflit ouvert ». Pour illustrer ce type de stratégie, le Chef d'État-major des armées a mentionné la mise à mal de la cohésion nationale, ce qui passe

[10] **Olivier de Maison Rouge,** Le droit du renseignement. Renseignement d'État; Renseignement économique, LexisNexis, 2016

[11] **État-major des armées. 2021.** Vision stratégique du Chef d'État-major des armées. [En ligne] octobre 2021. [Consulté le 25 mars 2022.] https://www.defense.gouv.fr/sites/default/files/ema/211022_EMACOM_VisionStrategiqueCEMA_FR_Vdef_HQ%20%282%29.pdf.

notamment par des attaques informationnelles, dans le but d'affaiblir le pays en interne. Pour faire face à ces menaces nouvelles, Thierry Burkhard préconise notamment de mieux connaître les stratégies, ce qui implique une phase d'analyse stratégique, de l'ennemi pour mieux les contrer.

1.3. De la guerre à la guerre économique

Ces nouvelles menaces, émanant du monde immatériel, ont finalement modernisé le cadre d'exercice de la "guerre" qui s'emploie aussi dans la sphère économique et informationnelle. Comme évoqué précédemment, la révolution de l'information bouleverse totalement l'ensemble des cadres conceptuels qui régissaient tant nos comportements d'humains que notre manière de faire de la politique, d'envisager la stratégie ou même de faire la guerre. D'ailleurs, cette dernière n'est plus le pré-carré des seules armées mais se joue également de manière asymétrique (État versus groupes non-étatiques…) ou encore sur les terrains de l'économie ou du droit. C'est la "guerre économique" qui s'illustre chaque jour dans l'actualité alors que la compétition s'intensifie à l'échelle mondiale. La guerre économique peut se résumer comme étant un affrontement entre les hommes pour capter les ressources.

En ce sens, elle a toujours existé dans l'histoire de l'humanité puisque dès le paléolithique, les hommes se sont fait la guerre pour le contrôle des ressources naturelles. Dans la 3ème édition du Manuel d'Intelligence économique, écrit sous la direction de Christian Harbulot, Ali Laïdi, définit la guerre économique de manière beaucoup plus précise :

« La guerre économique est l'utilisation de la violence, de la contrainte et de moyens déloyaux, ou illégaux, pour protéger ou conquérir un marché, gagner ou préserver une position dominante qui permet de contrôler abusivement un marché. La guerre économique s'exerce en temps de guerre comme de paix. Elle est pratiquée par les États, les entreprises, les associations et même les individus. Sachant que rien n'échappe à la marchandisation dans un monde néolibéral, la guerre économique s'applique aussi bien à tous les produits et services qu'à tous les biens immatériels, comme les pensées (guerre des idées), les croyances (guerre des Églises) et la connaissance (guerre cognitive). La politique n'a jamais eu le monopole de la violence. La violence a toujours existé dans le champ économique »[12].

La guerre ne se situe pas uniquement dans le domaine physique mais s'est aussi déplacée sur le terrain de l'immatériel et plus particulièrement autour de la donnée. Toutefois, les modes d'affrontement des mondes matériel et immatériel connaissent des similitudes avec les techniques de l'espionnage industriel, des combats juridiques ou encore les détournements de brevet. En revanche, le monde immatériel connaît également sa propre logique conflictuelle : il ne s'agit plus seulement de chercher les informations stratégiques des concurrents mais de divulguer un maximum celles-ci. Par ailleurs, ces données disponibles à grande échelle ont également fait émerger le sujet de l'influence. En atteignant la suprématie informationnelle, il est alors aisé de devenir un leader d'opinion et ainsi d'orienter la population dans divers domaines comme les choix de consommation ou encore l'opinion sur des sujets sociétaux ou politiques.

[12] **LAÏDI Ali, Une histoire de la guerre économique in Christian Harbulot, Manuel d'Intelligence économique. 3ème édition, 2019**, PUF, 43-54

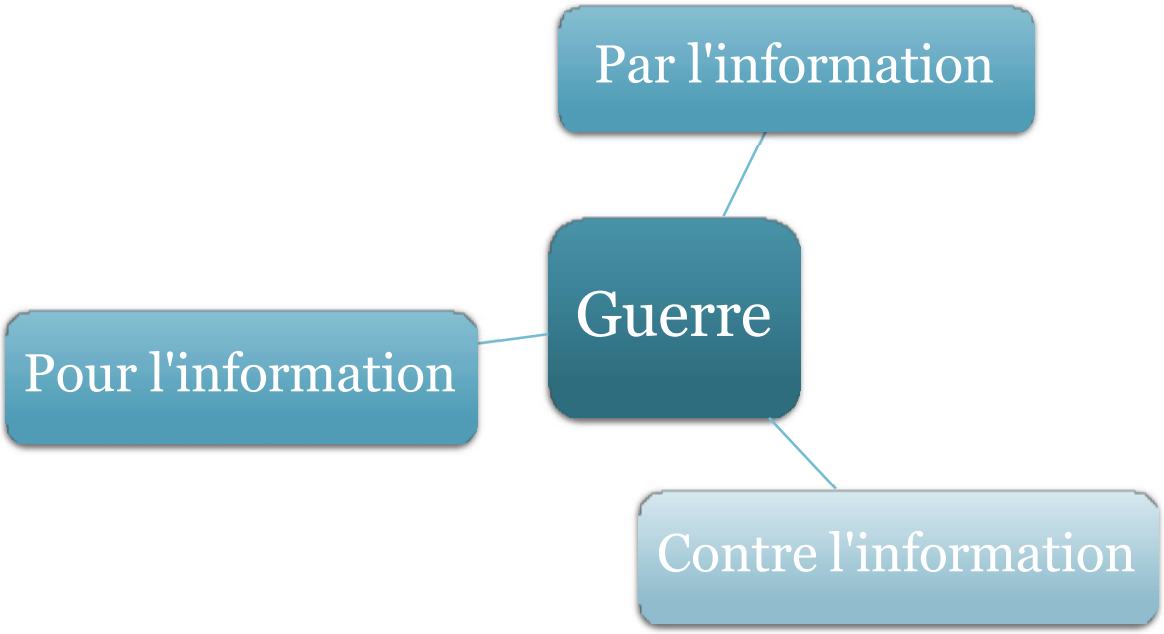
1.4. La guerre de l'information

Dans le prolongement de l'intelligence économique et de la guerre économique, le pendant informationnel est arrivé avec "la guerre de l'information". Pour mieux appréhender les enjeux qui se cachent derrière, il apparaît nécessaire de s'attarder sur leur définition et leur évolution. En effet, la guerre de l'information est devenue un objet médiatique de premier plan alors que ses manifestations et ses acteurs se multiplient et se diversifient. En effet, si le concept, qui est d'origine militaire, n'est pas nouveau, il s'est renouvelé à l'aune du développement des NTIC. En effet, les vecteurs de ces opérations de guerre de l'information sont beaucoup plus nombreux. Tout au long du XXème siècle, la guerre de l'information a été employée sous la forme d'opérations de propagande ou encore de désinformation durant la Seconde Guerre mondiale et la Guerre froide notamment. L'enjeu a toujours été de détenir l'information afin de « mener la danse » et *in fine* détenir le pouvoir. Le développement des NTIC, qui a entraîné la multiplication des données disponibles, a clairement décuplé et facilité le recours à la guerre de l'information.

C'est pourquoi il apparaît nécessaire de définir le concept de manière exhaustive à l'heure de l'explosion de son usage et d'une prise de conscience de la menace portée par celle-ci par les autorités publiques. Cette prise de conscience étatique s'est d'ailleurs matérialisée par la création de Viginum à l'été 2021. Cette nouvelle entité du SGDSN, qui dépend du Premier ministre, est chargée de lutter contre les manipulations de l'information émanant de l'étranger.

La guerre de l'information est définie, sur le site du Portail de l'IE, comme une « combinaison d'actions humaines ou technologiques destinées à l'appropriation, la destruction ou la modification de l'information »[13]. En résumé, il s'agit d'un concept large auquel on peut rattacher l'ensemble des actions visant à compromettre des données dans un but malveillant.

Christian Harbulot, spécialiste français de l'intelligence économique et de la guerre de l'information, a élaboré une grille de lecture à trois niveaux : Par/Pour/Contre.



Les 3 strates de la guerre de l'information élaborées par Christian Harbulot

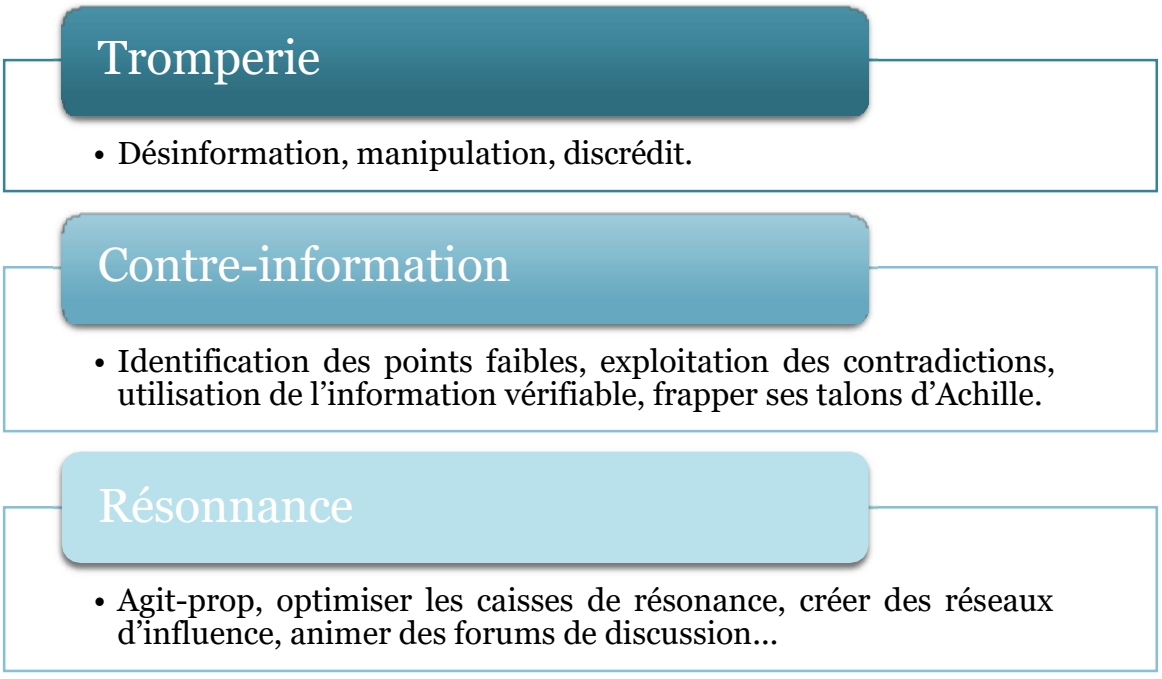
[13] **Centre de ressources et d'information sur l'intelligence économique et stratégique.** Guerre de l'information. *Portail de l'IE*. [En ligne] [Consulté le : 25 mars 2022.] https://portail-ie.fr/resource/glossary/97/guerre-de-linformation

- **Guerre par l'information :** il s'agit de manipuler, façonner l'information en vue d'atteindre un objectif fixé en vue d'exercer une certaine influence voire de brouiller la prise de décision des concurrents;

- **Guerre pour l'information :** il s'agit de maîtriser les canaux de diffusion de l'information. Dans ce cadre, l'objectif est de connaître des informations le premier et aussi d'en détenir certaines que les concurrents n'auront pas;

- **Guerre contre l'information :** il s'agit de limiter l'accès du concurrent à l'information dans le but d'avoir un temps d'avance et in fine opérer un certain contrôle dessus. Le « stade ultime » de la guerre contre l'information, il peut être défini comme étant l'agnotologie. Ce terme a été initié par l'historien des sciences américain Robert Proctor au milieu des années 1990. Il se diffuse ensuite via les débats publics et la presse dès 2003. L'agnotologie désigne la manière dont l'ignorance peut être entretenue ou produite par divers procédés tels que la soustraction d'informations, la destruction d'informations ou encore le secret.

De ces trois strates de la guerre de l'information découlent une multitude de techniques. Dans le domaine économique, Christian Harbulot, a établi 3 catégories d'opérations de guerre de l'information[14] :



Les 3 catégories de la guerre de l'information déterminées par Christian Harbulot

[14] **HARBULOT, Christian. 2001.** Les principes de la guerre de l'information. *Infoguerre*. [En ligne] 14 novembre 2001. [Consulté le 25 mars 2022.] https://www.ege.fr/infoguerre/2001/11/les-principes-de-la-guerre-de-l-information.

1.5. PME/ETI : tous concernés !

Désormais, le sujet est devenu familier à la population tant les sujets autour de ces manipulations de l'information et son pendant inverse qu'est le « fact-checking » se sont multipliés au cours de ces dernières années. En revanche, les sujets traitent essentiellement de cet affrontement au niveau interétatique.

Or, les opérateurs privés sont également parties prenantes à cette guerre. Si les grands groupes sont largement conscients et proactifs sur les défis et les dangers que posent ces sujets identifiés de longue date comme étant stratégiques, la question est beaucoup moins adressée par les PME et ETI. La sensibilisation, sur ces sujets pourtant stratégiques et gages de pérennité, prospérité voire de survie pour l'entreprise est très faible. Les raisons peuvent être diverses et variées : manque de temps, manque d'intérêt, manque de culture stratégique, manque de moyens…

Pourtant ne pas prendre en considération ce risque comporte une menace majeure pour les entreprises, quels que soient leur taille et leur domaine d'activité. A l'heure d'internet et des réseaux sociaux, chaque entreprise est une victime potentielle.

L'information est devenue un levier stratégique dont il faut apprendre à tirer profit au maximum mais aussi à se protéger. Faire l'impasse sur l'information et son traitement génère un handicap pour l'entreprise en la privant potentiellement de sources de développement voire en mettant sa survie en jeu. Dans le monde d'aujourd'hui, il n'est plus possible de faire l'impasse sur ce domaine. Désormais, il ne s'agit plus d'être à l'avant-garde dans le traitement de l'information mais bien de l'intégrer à sa stratégie d'entreprise pour rattraper son retard. L'information et son traitement sont devenus indispensables au bon fonctionnement d'une entreprise tant pour maximiser sa compétitivité, qu'améliorer son fonctionnement interne que de se prémunir d'une éventuelle attaque. En somme, il s'agit d'être le mieux informé possible pour faire des choix stratégiques éclairés sur les courts, moyens et longs termes. Pour de nombreuses entreprises, l'information est encore considérée comme un « OVNI », « gadget » sans réelle utilité. Par manque de temps, d'intérêt ou par simple ignorance, de nombreuses PME et ETI se privent de cette ressource pourtant essentielle à leur pérennité. La sensibilisation à cette thématique est donc essentielle : l'IE n'est plus un domaine réservé aux seules grandes entreprises multinationales ou à quelques secteurs stratégiques tels que le nucléaire, les énergies fossiles ou encore l'armement. Le développement des NTIC a fait émerger des problématiques nouvelles telles que l'E-réputation qui concernent l'ensemble des acteurs, domaines et tailles confondus. Le simple restaurateur pourra ainsi trouver sa réputation ternie sur Internet par des clients mécontents ou le restaurateur du village d'à-côté, de la rue voisine sous couvert d'anonymat.

De ces bouleversements résulte l'émergence de nouvelles menaces dont il convient, dans un premier temps, de prendre conscience pour mieux les affronter. Dans un second temps, il faut alors adapter son fonctionnement et ses pratiques pour en faire un levier stratégique de premier plan. Il s'agit de s'adapter et de faire preuve d'agilité face à une menace mouvante et en constante évolution. D'autre part, il faut réaliser une véritable « révolution culturelle » tant la culture de l'information et du renseignement est très faible en France.

L'intelligence économique, au sens large, est une matière cruciale pour les entreprises et ce à plusieurs titres. Elle est à la fois un levier de croissance, mais aussi un moyen de se prémunir d'éventuelles attaques ou « coups bas » de concurrents. Elle permet également de bien connaître l'écosystème dans lequel l'entreprise évolue. Enfin, elle peut aussi être utilisée en vue de mieux connaître ses propres faiblesses et atouts en vue d'améliorer ses performances ou de se lancer dans de nouveaux challenges.

En somme, pour une entreprise, la mise en place d'une stratégie d'intelligence économique peut générer des avantages compétitifs pour l'entreprise et ainsi orienter au mieux sa stratégie en fonction des informations récoltées.

L'IE peut être utilisée selon quatre modes : défensif ; offensif ; dissuasif ; informatif. Les buts de la mise en place d'une stratégie d'intelligence économique peuvent être résumés comme suit :

- Maîtriser et protéger l'information stratégique.
- Produire des informations via l'analyse et l'anticipation.
- Pérenniser son activité.
- Se développer son activité.
- Faire apparaître les opportunités, les faiblesses, les angles-morts qu'il faut exploiter ou améliorer.
- Conquérir de nouveaux marchés.
- Rendre visible les menaces et les réduire.

La stratégie d'entreprise selon Michael E. Porter est « l'art de se construire des avantages durablement rentables par rapport à son environnement par la réduction de l'incertitude, des innovations, des verrouillages, son accroissement, des synergies, la flexibilité »[1].

Les avantages de la mise en place d'une stratégie d'IE peuvent être déclinés comme suit :

- Développer une « vision 360° » de son environnement permet d'adapter au mieux sa prise de décision, sa stratégie.
- Réactivité.
- Pro-activité.
- Anticipation.
- Connaître ses faiblesses et ses atouts.

Pour tirer parti au maximum d'une stratégie d'Intelligence économique, il convient pour l'entreprise de faire preuve d'une forte réactivité pour manier les informations récoltées et les incorporer dans sa stratégie. En effet, récolter une masse d'informations stratégiques sans les utiliser ni les incorporer à sa stratégie n'apporte aucun avantage à l'entreprise. Les informations récoltées doivent être analysées pour ensuite orienter la prise de décision stratégique.

En résumé, la mise en place d'une politique d'intelligence économique revient à appliquer la boucle Observation-Orientation-Décision-Action, dite OODA.

La boucle OODA

Par ailleurs, outre l'agilité, une démarche réussie d'intelligence économique nécessite l'adhésion totale de l'ensemble des personnes impliquées. L'IE est avant tout une démarche collective. Enfin, il est également nécessaire de s'intéresser aux questions interculturelles. En effet, connaître la culture de ses clients, de ses concurrents est primordial afin de ne pas miser sur des réactions, comportements selon ses propres codes culturels.

1.6. Cas d'usages

Pour prendre conscience de la réalité de ces menaces qui pèsent également sur les PME et ETI, il est intéressant de les illustrer par des exemples concrets. Néanmoins, la sensibilité de ces sujets et le fait qu'être victime de ce type d'attaque envoie une mauvaise image de l'entreprise, il est difficile d'obtenir des cas réels. Sur ce sujet, une certaine omerta règne quels que soit la taille de l'entreprise et son domaine d'activité.

En revanche, la DGSI diffuse mensuellement un document destiné à sensibiliser les entreprises sur l'ingérence économique. Intitulé « Flash ingérence », le document présente à chaque fois des cas concrets, sans citer le nom des entreprises concernées, et des recommandations pour faire face aux menaces mentionnées. Parmi les cas cités, se trouvent de nombreuses PME et start-up, moins sensibilisées aux problématiques de guerre économique et de guerre de l'information.

Honorabilité et réputation des partenaires commerciaux[15] :

« Une PME française, produisant notamment des biens soumis à des réglementations internationales à l'export, a été contactée par une entreprise étrangère se présentant comme un « intermédiaire » de son client habituel pour gérer entièrement une commande. La marchandise a été envoyée, le règlement reçu. Or, la PME s'est rendu compte que son client habituel n'avait passé aucune commande par le biais d'un intermédiaire. La société pourrait être mise en difficulté par la livraison de biens non autorisés à un tiers jusqu'alors inconnu. »

[15] **Ministère de l'Intérieur. 2021.** Ingérence économique - De l'importance de contrôler l'honorabilité et la réputation de ses partenaires commerciaux. [En ligne] mai 2021. [Consulté le 25 mars 2022.] Flash DGSI #74. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Contr%C3%B4le%20de%20l%27honorabilit%C3%A9%20et%20de%20la%20r%C3%A9putation%20de%20ses%20partenaires%20commerciaux-Mai%202021.pdf.

Hébergement de données sur le Cloud[16] :

« Différents cas ont été rapportés : fuite de données stratégiques disposées sur le Cloud après que l'un des prestataires du Cloud ait été ciblé par une attaque cyber (ransomware) ; une entreprise ayant hébergés ses données à l'étranger –potentiellement cible d'opérations de captation- demande à son prestataire de les transférer sur des serveurs exclusivement situés en France pour protéger ses données par les lois françaises. Le prestataire accepte mais impose un délai de 2 ans pour effectuer la migration. Avec la crise sanitaire, le délai a été allongé de 2 ans supplémentaires tandis que l'entreprise a dû stocker d'autres données stratégiques sur le Cloud étranger pour poursuivre son activité lors des confinements. »

Partenariat déséquilibré avec un acteur étranger[17] :

« Une PME française, ayant un savoir-faire de pointe et des difficultés financières, établit un partenariat avec un groupe international. En échange d'un soutien financier, la PME offre un soutien technique. Or, le groupe s'est petit à petit approprié le savoir-faire de la PME et le développe désormais en interne. Le groupe international est désormais un concurrent direct de la PME et est en position avantageuse du fait des économies d'échelle qui lui permettent de proposer des prix plus compétitifs. »

Entretiens rémunérés[18] :

« Des cabinets d'intelligence économique étrangers, réputés être proches des autorités de leur pays, ont contacté, à quelques semaines d'intervalle, le dirigeant d'une PME française parmi les leaders européens dans son domaine d'activité. Chaque demande, contre rémunération, aurait permis de dévoiler des informations stratégiques de l'entité visée. »

[16] **Ministère de l'Intérieur. 2020.** Ingérence économique - Les risques liés à l'hébergement de données dans le Cloud. [En ligne] novembre 2020. [Consulté le 25 mars 2022.] Flash DGSI #69. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Risques%20li%C3%A9s%20%C3%A0%20l%27usage%20du%20Cloud%20Novembre%202020_0.pdf.

[17] **Ministère de l'Intérieur. 2020.** Ingérence économique - Les risques de captation d'informations liés aux partenariats déséquilibrés avec des acteurs étrangers. [En ligne] décembre 2020. [Consulté le 25 mars 2022.] Flash DGSI #70. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Les%20risques%20li%C3%A9s%20aux%20partenariats%20d%C3%A9s%C3%A9quilibr%C3%A9s%20avec%20des%20acteurs%20%C3%A9trangers%20d%C3%A9loyaux%20d%C3%A9cembre%202020.pdf.

[18] **Ministère de l'Intérieur. 2021.** Ingérence économique - Questionnaires et entretiens rémunérés. [En ligne] décembre 2021. [Consulté le 26 mars 2022.] Flash DGSI #79. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-12/Questionnaires%20et%20entretiens%20r%C3%A9mun%C3%A9r%C3%A9s-%20d%C3%A9cembre%202021.pdf.

Atteinte à la réputation[19] :

« Une PME française, offrant des produits utilisés dans des industries sensibles et nécessitant des certifications, est bien implantée à l'étranger. En quelques mois, la PME perd plusieurs contrats sur un marché étranger. Les contrats ont tous été remportés par une entreprise locale créée récemment. A posteriori, la PME a découvert que l'entreprise locale a mené une opération de dénigrement à son encontre en affirmant aux clients que les produits français avaient perdu leurs certifications. Elle a alors déployé un large plan de communication pour rétablir sa réputation et rassurer les clients. »

Par ailleurs, certains professionnels de la gestion de crise ou de l'IE peuvent également rapporter quelques cas qu'ils ont eu à gérer. Ainsi, le fondateur de l'agence de communication de crise LaFranchCom a évoqué dans la presse le cas de l'un de ses clients[20]. Ce dernier, un petit imprimeur du sud-ouest de la France, a été victime d'une campagne mensongère opérée par l'un de ses concurrents. Le concurrent faisait courir le bruit que l'imprimeur était en liquidation judiciaire. Cela a entraîné des diminutions de commandes et de nombreuses annulations ainsi que de nombreuses inquiétudes chez les salariés. Une fois le concurrent démasqué, il a fallu rassurer employés, banquiers, fournisseurs et clients (pour plus de détails, se référer au chapitre relatif au cadre législatif et au chapitre relatif à l'Infox et aux tentatives de déstabilisation).

1.7. Environnement et cadre législatif

Le présent paragraphe tente de donner un aperçu du cadre législatif inhérent à la thématique traitée. Sans être absolument exhaustif, il a pour objectif de présenter le cadre légal des différentes méthodologies et outils décrits dans le document, utilisés comme outils défensifs et/ou offensifs dans le contexte de guerre informationnelle.

Nous allons le voir, plusieurs règles strictes encadrent, par exemple, les investigations en ligne ou la collecte de données numériques, pouvant être réalisées par une cellule de veille par exemple. Mais nous le verrons aussi, l'environnement législatif est très mouvant et de nombreuses jurisprudences existent et sont soumises à interprétation. Il est donc nécessaire de connaître ces dernières pour pouvoir apprécier, au cas par cas, la légalité des actions entreprises.

[19] **Ministère de l'Intérieur. 2021**. Ingérence économique - Le dénigrement commercial, facteur de pertes de marchés et déstabilisation financière. [En ligne] juin 2021. [Consulté le 26 mars 2022.] https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Ing%C3%A9rence%20d%C3%A9nigrement%20commercial-Juin%202021.pdf.

[20] **VILLARS, Nathalie. 2021.** Artisans, PME, médecins… quand les rumeurs ruinent nos entrepreneurs. *Capital.* [En ligne] 19 avril 2021. [Consulté le 26 mars 2022.] https://www.capital.fr/votre-carriere/artisans-pme-medecins-quand-les-rumeurs-ruinent-nos-entrepreneurs-1400414.

1.7.1. Législation française et sanctions en matière d'intrusion informatique

La législation française est assez claire sur le caractère illicite des intrusions sur des systèmes d'information. Les infractions en la matière sont décrites dans l'article 323 du Code Pénal, en particulier dans les articles 323-1, 323-2 et 323-3 qui énoncent plusieurs principes de base :

Article 323-1 du code pénal[21] :

« Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende. »

Article 323-2 du Code Pénal[22] :

« Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

Article 323-3 du code pénal[23] :

« Le fait d'introduire frauduleusement des données dans un système de traitement automatisé, d'extraire, de détenir, de reproduire, de transmettre, de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 150 000 € d'amende.

Lorsque cette infraction a été commise à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'État, la peine est portée à sept ans d'emprisonnement et à 300 000 € d'amende. »

D'abord, le périmètre applicable de ces dispositions concerne tout « système de traitement automatisé de données ». Par ce terme, le législateur inclut naturellement l'informatique « classique », à savoir les

[21] **Code pénal, article 323-1, version en vigueur depuis le 27 juillet 2015**, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/, consulté le 17 avril 2022

[22] **Code pénal, article 323-2, version en vigueur depuis le 27 juillet 2015**, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939443, consulté le 17 avril 2022

[23] **Code pénal, article 323-3, version en vigueur depuis le 27 juillet 2015**, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939448, (consulté le 17 avril 2022)

ordinateurs ou systèmes d'informations, mais aussi les supports informatiques mobiles tels que les smartphones ou encore les périphériques de stockage tels que les clés USB ou disques durs externes.

Plusieurs comportements sont punis par ces dispositions :

- D'abord, l'accès frauduleux ou l'intrusion dans un système est puni. Il est entendu par frauduleux toute technique permettant de contourner les mécanismes de filtrage ou de sécurité en place pour parvenir à accéder au système. Par exemple, l'utilisation de la technique de la force brute (ou *Brute Force*) pour *cracker* le mot de passe d'un utilisateur et accéder ainsi au système. Cette disposition est aggravée si l'intrusion aboutit à une suppression ou altération des données, si le fonctionnement du système est endommagé ou si les actions sont effectuées sur un système fourni par l'État.

- Ensuite, la notion de « maintien » est elle aussi punie, même si l'accès initial n'a pas été réalisé de manière frauduleuse. Par exemple, si un salarié quitte une société mais que ses accès vers le système d'information ne lui ont pas été retirés, il lui est interdit de se maintenir sur le système, tout en sachant ne plus théoriquement y avoir droit. Dans ce cas, il n'y a pas d'intrusion, puisque le salarié utilise un accès légitime, mais le maintien reste quant à lui illicite. De la même manière, si un utilisateur, en visitant l'extranet d'une entreprise, accède à son intranet car un pont entre les deux plateformes n'a pas été correctement sécurisé, l'utilisateur qui a conscience d'être sur l'intranet n'aura pas le droit de s'y maintenir et devra immédiatement s'en déconnecter.

- Aussi, toute modification, extraction ou injection de données de manière illicite est elle aussi punie. A noter, la notion de « vol de données » n'est pas reconnue par le droit français, mais est couverte par la disposition relative à « l'extraction » de ces dernières depuis un système automatisé de traitement de données

- Enfin, le fait « d'entraver » le fonctionnement d'un système est lui aussi puni. Instinctivement et pour illustrer cette disposition, on pourrait penser aux cyberattaques créées spécialement pour endommager le fonctionnement du système, ou attaques dites de « Déni de Service » (DDoS). Cependant, une extraction massive de données sur système, réalisée de manière légitime mais causant un ralentissement du système pourra, elle aussi, rentrer dans une telle disposition. Il est donc important de la mentionner. Dans cette notion, c'est plutôt la notion de « dommage collatéral » qui est soulignée.

De manière plus indirecte, l'article 323-3-1 du Code Pénal indique qu'il n'est pas non plus autorisé de fournir ou diffuser des informations ou outils pouvant permettre de commettre les infractions mentionnées ci-dessus.

Bien sûr, cette disposition fait exception des « motifs légitimes », en particulier relatifs à la sécurité ou la recherche en sécurité informatique. En effet, le test d'intrusion (ou *penetration testing*) n'est pas interdit par la législation mais nécessite une contractualisation entre l'auditeur ou le chercheur en sécurité et le client audité, responsable du système testé.

Article 323-3-1[24] du Code pénal :

« Le fait, sans motif légitime, notamment de recherche ou de sécurité informatique, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

En matière de sanction, comme nous venons de le voir au travers des différents articles, la législation prévoit des peines importantes et ces infractions relèvent du pénal. Il est cependant important de noter que si ces faits sont commis par une entreprise (ou de manière globale une personne morale), les sanctions sont beaucoup plus sévères et peuvent conduire, entre autres, à une interdiction d'exercer pour le(s) dirigeant(s) de l'entreprise concernée. Les dispositions prises par le législateur à l'égard des personnes morales est détaillé dans l'article 323-6 du Code Pénal.

Article 323-6 du Code pénal[25] :

« Les personnes morales déclarées responsables pénalement, dans les conditions prévues par l'article 121-2, des infractions définies au présent chapitre encourent, outre l'amende suivant les modalités prévues par l'article 131-38, les peines prévues par l'article 131-39.

L'interdiction mentionnée au 2° de l'article 131-39 porte sur l'activité dans l'exercice ou à l'occasion de l'exercice de laquelle l'infraction a été commise. »

1.7.2. Législation relative aux bases de données

Le droit en matière de bases de données en France est encadré par les articles L342-1 et L342-2 du code de la propriété intellectuelle (CPI) comme suivant.

Article L342-1 du code de la propriété intellectuelle[26] :
« Le producteur de bases de données a le droit d'interdire :

1. *L'extraction, par transfert permanent ou temporaire de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu d'une base de données sur un autre support, par tout moyen et sous toute forme que ce soit ;*
2. *La réutilisation, par la mise à la disposition du public de la totalité ou d'une partie qualitativement ou quantitativement substantielle du contenu de la base, quelle qu'en soit la forme. »*

[24] **Code pénal, article 323-3-1, version en vigueur depuis le 20 décembre 2013**, modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345220, consulté le 17 avril 2022

[25] **Code pénal, article 323-6, version en vigueur depuis le 14 mai 2009**, modifié par LOI n°2009-526 du 12 mai 2009 - art. 124, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020630782, consulté le 17 avril 2022

[26] **Code de la propriété intellectuelle, article L342-1, version en vigueur depuis le 01 janvier 1998**, création Loi n°98-536 du 1 juillet 1998 - art. 5 () JORF 2 juillet 1998 en vigueur le 1er janvier 1998, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006279247, consulté le 17 avril 2022

Ces droits peuvent être transmis ou cédés ou faire l'objet d'une licence. Le prêt public n'est pas un acte d'extraction ou de réutilisation.

Article L342-2 du code de la propriété intellectuelle[27] : *« Le producteur peut également interdire l'extraction ou la réutilisation répétée et systématique de parties qualitativement ou quantitativement non substantielles du contenu de la base lorsque ces opérations excèdent manifestement les conditions d'utilisation normale de la base de données. »*

Cependant pour Eric Barbry [28], ce droit est relativement restrictif dans la définition de la base de données. Son détenteur doit en effet démontrer un investissement important ayant permis la construction de la base pour se prétendre être couvert par cette législation. De manière générale ce droit est souvent associé aux articles du code pénal précédemment évoqué pour monter un dossier en cas d'intrusion mais est plus rarement utilisé de manière unitaire.

1.7.3. Législation relative à la protection des données personnelles

1.7.3.1. La Commission Nationale de l'Informatique et des Libertés (CNIL)

En France, c'est la CNIL, autorité administrative indépendante existant depuis 1978, qui a la charge, entre autres, de la protection des données personnelles. Il est entendu par « données personnelles », toujours selon la CNIL, « *toute information se rapportant à une personne physique identifiée ou identifiable* »[29]. La subtilité résidant dans cette définition réside dans son périmètre. En effet, elle ne concerne pas seulement les données permettant d'identifier de manière directe une personne, telle que son nom ou prénom, mais aussi toute donnée pouvant permettre de l'identifier de manière indirecte.

La CNIL fait appliquer plusieurs réglementations aux entreprises et organisations françaises, à l'image de l'emblématique RGPD Européen, comme nous le verrons un peu plus tard. Au-delà de l'aspect préventif et pédagogique, la CNIL inflige à certaines entreprises qui ne respectent pas leurs obligations en la matière des sanctions financières. La récente sanction[30] d'1,5 millions d'euros à l'encontre de la société Dedalus Biologie pour la fuite de données médicales de près de 500 000 personne illustre bien ce rôle.

---

[27] **Code de la propriété intellectuelle, article L342-2, version en vigueur depuis le 01 janvier 1998**, Création Loi n°98-536 du 1 juillet 1998 - art. 5 () JORF 2 juillet 1998 en vigueur le 1er janvier 1998, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006279250/, consulté le 17 avril 2022

[28] **BARBRY Eric. 2020.** Risques légaux pour la veille / investigation en ligne ? - Club OSINT & Veille AEGE / Cabinet Racine, Conférence TVAEGE [en ligne], 25 octobre 2020 [consulté le 17 avril 2022], disponible à l'adresse : https://www.youtube.com/watch?v=to6c7wGXhAc,

[29] **CNIL. 2021.** RGPD : de quoi parle-t-on ? [En ligne] 2021. [Consulté le 15 avril 2022.] https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on .

[30] **CNIL. 2022.** Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE. [En ligne] 21 avril 2022. [Consulté le 05 mai 2022.] https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie .

1.7.3.2. Législation française en matière de données personnelles

A niveau national, la législation française inclut une disposition punissant sévèrement la collecte de données personnelles de manière illicite :

Article 226-18 du Code pénal[31] : *« Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de cinq ans d'emprisonnement et de 300 000 € d'amende. »*

Cette loi, dite « de 1978 » ou « Informatique & Liberté » a cependant une limite puisqu'elle inclut la notion de caractère illicite (« moyen frauduleux ») de la collecte des données personnelles. On peut ainsi la considérer comme une aggravation de l'intrusion par une collecte d'informations personnelles, plus qu'une loi sur la protection des données à caractère personnel à part entière.

Au niveau européen, c'est le Règlement Général sur la Protection des données (RGPD) qui vient, depuis 2016, compléter cette disposition du code pénal.

1.7.3.3. Le Règlement Général sur la Protection des données (RGPD)[32]

Le Règlement Général sur la Protection des Données, ou RGPD a été voté 27 avril 2016 et mis en application près de deux ans plus tard, le 25 mai 2018. Cette réglementation régule de manière globale la collecte et le traitement des données en Union Européenne. Il a notamment pour objectif une plus grande responsabilisation des entités ou entreprises collectant ou traitant de la donnée personnelle et accroît le rôle de la CNIL et de ses homologues européens.

Le RGPD s'applique donc aux données personnelles, que nous avons définies au chapitre ci-avant comme toute donnée permettant d'identifier une personne de manière directe ou indirecte. La notion de « traitement » inclut les actions suivantes, qu'elles soient réalisées de manières manuelles, automatisées ou semi-automatisées : *« le collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction »*

Sont concernées par le RGPD toute personne (physique, morale, sous-traitants) réalisant ces traitements. Les sociétés dont le siège social est établi en Union Européenne (UE) sont bien sûr concernées, mais pas seulement. Même les sociétés établies en dehors de l'UE mais qui fournissent des biens et services à des clients établis en UE sont concernés par le RGPD, tels que les sites de e-commerce ou fournisseur de services d'hébergement *Cloud*.

[31] **Code pénal, article 226-18, version en vigueur depuis le 07 août 2004**, modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417968/, [consulté le 17 avril 2022]

[32] **DE MAISON ROUGE Olivier. Note - Guide d'application du Règlement européen (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personne**l. Support de cours Ecole de Guerre Economique. 2022, p.32

Le RGPD regroupe plusieurs mesures emblématiques pour parvenir à ses objectifs, parmi lesquelles :

- L'obligation de **demander le consentement** de la personne concernée (sauf cas particuliers, tels que la conservation des intérêts vitaux de la personne) avant de procéder à tout traitement de ses données personnelles, ou de rendre ces dernières accessibles à un nombre indéterminé de personnes physiques.

- L'obligation de **nommer un Délégué à la Protection des Données (DPO)**, interne ou externe à l'entreprise, assurant la conformité de l'entreprise avec le RGPD.

- Obligation d'**informer la personne concernée** notamment sur la nature des traitements, le contact du DPO, la durée de conservation des données, ainsi que les droits de la personne : Droit d'accès aux données ; Droit de rectification de données potentiellement inexactes ; Droit à l'effacement ou « droit à l'oubli », en cas notamment de retrait du consentement au traitement, en dehors des exceptions prévues ; Droit à la limitation du traitement ; Droit de s'opposer au traitement ; Droit à la portabilité des données ; Droit à retirer son consentement ; Droit à effectuer une réclamation (auprès de la CNIL).

- L'obligation pour le responsable du traitement des données de **notifier la CNIL** dans les 72 heures suivant la prise de connaissance d'une violation de données en indiquant quelles données ont été compromises et en quelle quantité. Le cas échéant l'entreprise devra prévenir les personnes directement impactées ou, à défaut, effectuer une communication publique.

- L'obligation pour le responsable du traitement des données de **prendre des mesures de sécurité** pour garantir la confidentialité, intégrité et disponibilité des données collectées, en particulier par la réalisation d'analyses de risques et d'impacts et la mise en œuvre de mesures techniques ou organisationnelles.

- La **tenue d'un registre de traitement**, indiquant les coordonnées de responsables, les traitements, les destinataires éventuels des données, les mesures de protection et d'effacement des données.

- L'encouragement pour les entités traitant de la donnée de mettre en place une **posture de « *privacy by design* »** : anonymisation des données, limitation de leur collecte et leur conservation au strict nécessaire, limitation des destinataires, établissement d'un référentiel de sécurité applicable, etc.

- **L'obligation pour les sous-traitants** de prendre des mesures équivalentes sur la protection des données personnelles, et l'obligation de collaborer avec la CNIL et le responsable du traitement des données.

Le RGPD constitue un texte très fort de l'arsenal législatif sur la protection des données personnelles, puisqu'une entreprise qui ne le respecte pas peut se voir infliger des sanctions pouvant aller jusqu'à 10 millions d'euros ou 4% de son chiffre d'affaires annuel mondial. Au-delà des sanctions, les personnes ayant subi des préjudices relatifs au non-respect du RGPD par un responsable de traitement (ou un de ses sous-traitants) sera en mesure de demander des réparations à celui-ci.

1.7.4. Le secret des affaires

Le secret des affaires est encadré en France par la loi n° 2018-670 du 30 juillet 2018[33] et est inspirée[34] de la disposition du 8 juin 2016 prise par le législateur européen.

Avant ce texte, la France disposait déjà de législation sur le secret liée à certains secteurs. On pense notamment au secret médical, au secret défense, ou encore au secret bancaire. Pour les autres secteurs, le secret était assuré par la contractualisation et la signature d'accords de confidentialité (*Non-Disclosure Agreement*, *NDA*) par les parties entre elles. En 2018, le législateur est venu renforcer ces dispositions pour offrir aux entreprises une base juridique à la protection des informations sensibles et / ou stratégiques pour l'entreprise. Par ailleurs, les informations concernées par ce secret doivent remplir un certain nombre de critères, notamment d'avoir une valeur commerciale pour son détenteur, ne pas être facilement accessible et être suffisamment protégée, comme le stipule l'article L151-1 du code de commerce.

Article L151-1 du code de commerce[35] :
« Est protégée au titre du secret des affaires toute information répondant aux critères suivants :

1. *Elle n'est pas, en elle-même ou dans la configuration et l'assemblage exacts de ses éléments, généralement connue ou aisément accessible pour les personnes familières de ce type d'informations en raison de leur secteur d'activité ;*
2. *Elle revêt une valeur commerciale, effective ou potentielle, du fait de son caractère secret ;*
3. *Elle fait l'objet de la part de son détenteur légitime de mesures de protection raisonnables, compte tenu des circonstances, pour en conserver le caractère secret. »*

Article L151-2 du code de commerce[36] : « *Est détenteur légitime d'un secret des affaires celui qui en a le contrôle de façon licite* ».

Selon Eric BARBRY, il est important de noter que la notion de « protection raisonnable » reste relativement subjective pour chaque cas traité par la justice. De même, l'article L151-2 indique que seule la personne qui a licitement le contrôle de ces données en est le détenteur légitime.

Réciproquement, les articles L151-4 à L151-6 listent les cas qui ne rentrent pas dans cette disposition, c'est-à-dire les cas d'obtention illicite de ces informations soumises au droit des affaires. On peut synthétiser les modes d'obtention illicites par les points suivants :

- Accès ou copie non autorisé aux documents ou support contenant le secret ou permettant de le déduire

[33] **Légifrance. 2018.** LOI n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. [En ligne] 30 juillet 2018. [Consulté le 02 mai 2022.] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111 .

[34] **CCI Ile-de-France. 2020.** Secret des affaires - Comment bénéficier de la protection prévue par la loi du 30 juillet 2018 ? [En ligne] 04 décembre 2020. [Citation : 02 mai 2022.] https://www.cci-paris-idf.fr/sites/default/files/2020-12/guide-secret_des_affaires.pdf.

[35] Code de commerce, article L151-1, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266553/, consulté le 17 avril 2022

[36] code de commerce, article L151-2, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266557 , consulté le 17 avril 2022

- Utilisation de tout acte jugé “déloyal” ou contraire “aux usages” commerciaux pour obtenir l’information
- L’utilisation ou la divulgation du secret s’il a été obtenu de manière illicite (selon les moyens précisés ci-dessus)
- L’interdiction de toute production, vente, importation ou exportation de produits résultant de l’obtention illicite d’une information soumise au secret des affaires
- L’interdiction de l’obtention ou divulgation du secret si la personne le récupérant sait que cette information a été au préalable obtenue par un moyen illicite.

Article L151-4 du code de commerce[37] :

« L'obtention d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime et qu'elle résulte :

1. *D'un accès non autorisé à tout document, objet, matériau, substance ou fichier numérique qui contient le secret ou dont il peut être déduit, ou bien d'une appropriation ou d'une copie non autorisée de ces éléments ;*
2. *De tout autre comportement considéré, compte tenu des circonstances, comme déloyal et contraire aux usages en matière commerciale. »*

Article L151-5 du code de commerce[38] :

« L'utilisation ou la divulgation d'un secret des affaires est illicite lorsqu'elle est réalisée sans le consentement de son détenteur légitime par une personne qui a obtenu le secret dans les conditions mentionnées à l'article L. 151-4 ou qui agit en violation d'une obligation de ne pas divulguer le secret ou de limiter son utilisation.

La production, l'offre ou la mise sur le marché, de même que l'importation, l'exportation ou le stockage à ces fins de tout produit résultant de manière significative d'une atteinte au secret des affaires sont également considérés comme une utilisation illicite lorsque la personne qui exerce ces activités savait, ou aurait dû savoir au regard des circonstances, que ce secret était utilisé de façon illicite au sens du premier alinéa du présent article. »

Article L151-6 du code de commerce[39] :

« L'obtention, l'utilisation ou la divulgation d'un secret des affaires est aussi considérée comme illicite lorsque, au moment de l'obtention, de l'utilisation ou de la divulgation du secret, une personne savait, ou aurait dû savoir au regard des circonstances, que ce secret avait été obtenu, directement

[37] Code de commerce, article L151-4, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266563 , consulté le 17 avril 2022

[38] Code de commerce, article L151-5, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037266565/2021-07-13, consulté le 17 avril 2022

[39] Code de commerce, article L151-6, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266567/, consulté le 17 avril 2022

ou indirectement, d'une autre personne qui l'utilisait ou le divulguait de façon illicite au sens du premier alinéa de l'article L. 151-5. »

Il est à noter que ces dispositions sont soumises au droit civil et non pénal.

De l'autre côté, l'article L151-3, quant à lui, indique les modes licites d'obtention des données.

Article L151-3 du code de commerce[40] :

« Constituent des modes d'obtention licite d'un secret des affaires :

1. *Une découverte ou une création indépendante ;*
2. *L'observation, l'étude, le démontage ou le test d'un produit ou d'un objet qui a été mis à la disposition du public ou qui est de façon licite en possession de la personne qui obtient l'information, sauf stipulation contractuelle interdisant ou limitant l'obtention du secret. »*

Comme on peut le voir, cette dernière disposition précise bien que « l'observation, l'étude, le démontage ou le test » d'un produit est un mode d'obtention licite de l'information. Cependant, on peut se demander dans quelle mesure les informations sont réellement publiques ou non. Par exemple, si j'ai accès à une donnée publiée sur un réseau social par un personne avec qui je ne suis pas en contact : cette donnée a-t-elle été « mise à disposition du public » ? Nous reviendrons sur ce point central un peu plus tard, en nous concentrant sur le cadre des jurisprudences existantes en matière de veille ou d'investigation numérique.

1.7.5. Les actes de concurrence déloyale

En droit français, la concurrence déloyale est principalement basée sur des jurisprudences et fonde sur la notion de « responsabilité délictuelle » décrite à l'article 1240 du code civil[41] qui indique que « *Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer.* ». Pour être reconnus comme tel, un acte de concurrence déloyale doit réunir plusieurs critères[42]. Il doit d'abord y avoir la reconnaissance d'une faute par l'entreprise réalisant cet acte. L'acte doit aussi causer un préjudice et ce dernier doit être lié à la faute commise.

On trouve quatre types de concurrence déloyale, plus ou moins liées à l'environnement de la guerre informationnelle : le dénigrement, la confusion, la désorganisation ou le parasitisme économique. Les tribunaux de commerce ont la compétence pour juger ces affaires pour les commerçants, et ce sont les tribunaux judiciaires qui jugent ce type d'acte pour les non-commerçants.

[40] Code de commerce, article L151-3, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266559 , consulté le 17 avril 2022

[41] Code civil, Article 1240, Version en vigueur depuis le 01 octobre 2016, modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 2, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032041571/, consulté le 24 avril 2022

[42] **OOREKA Droit. 2022.** Concurrence déloyale. [En ligne] mai 2022. [Consulté le 05 mai 2022.] https://justice.ooreka.fr/astuce/voir/516991/concurrence-deloyale.

Le dénigrement, dont la qualification est sujette à plusieurs critères[43]. D'abord, l'auteur doit avoir l'objectif de nuire. Cette première composante doit en effet être qualifiée par une juridiction pour pouvoir qualifier le dénigrement. Ensuite, les propos doivent remplir trois conditions :

- Ils ont pour objectif de « *jeter le discrédit* » sur un produit et provoquer un sentiment défavorable à son égard
- Ils ne sont pas ou insuffisamment basés sur des faits
- Ils ne sont pas mesurés

Les notions de mesure et de base factuelle sont notamment jugées pour différencier un acte de dénigrement d'un simple acte de libre critique, qui lui est autorisé dans le cadre de la liberté d'expression. Ce sont donc ces deux principales composantes qu'il sera utile de juger pour apprécier un acte de dénigrement.

Le dénigrement peut s'appliquer pour toute entreprise et ne suppose pas que l'auteur du dénigrement et sa victime soient nécessairement en situation de concurrence. Attention cependant à ne pas confondre la notion de « dénigrement » avec la notion de « diffamation » qui, même si elle est aussi punie, concerne des personnes et non des produits ou entreprises.

Le parasitisme commercial a été défini par la Cour de cassation le 5 juillet 2016[44] comme le fait de « *tirer indûment profit du savoir-faire et des efforts humains et financiers consentis par une entreprise, victime des agissements de la personne qui usurpe la notoriété acquise par ce concurrent* ».

En d'autres termes, la notion de parasitisme commercial s'applique lorsqu'un individu ou une entreprise utilise l'image ou la notoriété d'une marque pour en tirer profit et se créer un avantage concurrentiel sans avoir eu à réaliser les investissements nécessaires. Ces actes peuvent entraîner des pertes de revenus pour l'entreprise qui en est la victime ou produire des dégâts en termes d'image.

La confusion est le plus souvent liée à l'utilisation ou la copie de signes distinctifs tels que le logo ou la marque pouvant semer la confusion dans l'esprit des clients à qui est adressé le message.

Enfin, **la désorganisation** consiste pour une entreprise à embaucher massivement des salariés de son concurrent dans le but de nuire à son organisation mais aussi récupérer pour son propre compte des savoir-faire détenus par ces employés.

Les méthodes permettant d'y parvenir peuvent potentiellement passer par l'utilisation du renseignement en source ouverte pour identifier les employés ou personnels stratégiques.

[43] **HAAS, Gérard et CADOT, Marie . 2021.** Dénigrement et pratique commerciale trompeuse : Yuka condamnée. *HAAS Avocats*. [En ligne] 2021. [Consulté le 05 mai 2022.] https://info.haas-avocats.com/droit-digital/denigrement-et-pratique-commerciale-trompeuse-yuka-condamnee.

[44] **Avocats Picovschi. 2021.** Concurrence déloyale et parasitisme. *Avocats-Picovschi.* [En ligne] 29 septembre 2021. [Consulté le 13 mars 2022.] https://www.avocats-picovschi.com/concurrence-deloyale-et-parasitisme_menu2_67_14.html.

1.7.6. Protection des lanceurs d'alerte

1.7.6.1. Loi dite « Sapin II » (2016)

Le législateur protège le statut de « lanceur d'alerte » en France depuis 2016 et le dispositif mis en place par la loi dite « Sapin II »[45]. En 2019, cette loi s'est aussi transposée au niveau européen, où une protection a été mise en œuvre pour tout « lanceur d'alerte » qui dénoncerait une éventuelle irrégularité vis-à-vis du droit européen.

Dans la loi « Sapin II », le lanceur d'alerte est défini comme « *une personne physique qui révèle ou signale, de manière désintéressée et de bonne foi, un crime ou un délit, une violation grave et manifeste d'un engagement international régulièrement ratifié ou approuvé par la France, d'un acte unilatéral d'une organisation internationale pris sur le fondement d'un tel engagement, de la loi ou du règlement, ou une menace ou un préjudice graves pour l'intérêt général, dont elle a eu personnellement connaissance.* »[46]

Si le lanceur d'alerte répond à cette définition, il ne sera pas pénalement répréhensible de la divulgation d'un secret protégé par la loi ou le secret des affaires. La divulgation doit cependant être « nécessaire » et « proportionnée », et suivre une démarche précise. Dans un premier temps, le lanceur d'alerte doit avertir son supérieur hiérarchique. Si celui-ci ne donne pas de réaction, il pourra remonter l'information auprès de l'autorité judiciaire ou administrative, ou un ordre professionnel compétent. C'est seulement si ces différentes entités ne réagissent pas « dans un délai raisonnable » ou si la non-divulgation du secret fait courir un danger imminent ou de représailles que l'information peut être rendue publique.

Au-delà des dispositions pénales, la loi protège le lanceur d'alerte en interdisant toute diffamation ou sanction de la part de l'entreprise à l'égard d'un lanceur d'alerte. Elle punit aussi toute entrave à la transmission ou la divulgation du secret en question.

1.7.6.2. Loi dite « Waserman » (2022)

Depuis juillet 2021 et la parution d'un rapport d'évaluation de la loi « Sapin II » sur la protection des lanceurs d'alerte, une nouvelle loi a vu le jour en mars 2022. Cette dernière, dite « loi Waserman » a pour but d'élargir les protections accordées à ces derniers.

Cette dernière inclut les dispositions suivantes :

- Clarification de la définition de lanceur d'alerte, en remplaçant la notion de « désintéressé » par « absence de contrepartie financière »
- Le lanceur d'alerte n'a plus besoin d'avoir personnellement connaissance des faits mais peut « signaler des faits qui lui sont remontés »
- Les faits remontés n'ont plus besoin de concerner une information sur un manquement à la législation mais peuvent aussi concerner des « tentatives de dissimulation » de ces dernières

[45] **Vie Publique. 2022.** Loi du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte. [En ligne] 22 mars 2022. [Consulté le 01 avril 2022.] https://www.vie-publique.fr/loi/282472-loi-21-mars-2022-waserman-protection-des-lanceurs-dalerte .

[46] **LOI n° 2016-1691 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique** (1), [En ligne] 9 décembre 2016, [consulté le 24 avril 2022] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528/

- Un nouveau statut de « facilitateur » est créé pour les personnes physiques (collègues par exemple) ou morales (syndicats par exemple)
- Le choix pour le lanceur d'alerte d'alerter en premier lieu sa hiérarchie ou une autorité externe compétente (pour éviter les représailles), avec l'appui du Défenseur des Droits
- Avance des frais de justice, dans certains cas précis

1.7.7. Législation internationale : les exemples du *Cloud Act* et du *Patriot Act*

Nous avons détaillé l'arsenal français et européen en matière de protection de l'information stratégique de l'entreprise (secret des affaires), des données personnelles (RGPD) ainsi que les moyens illicites de récupération d'information par l'intrusion sur un système de traitement de données.

Le panorama ne serait cependant pas complet si nous n'évoquions pas la question de la territorialité et l'extraterritorialité de certaines législations en vigueur dans des pays en dehors de la France et de l'Union Européenne. En matière de protection des données, deux lois américaines emblématiques méritent d'être mentionnées, à savoir le *Patriot Act* et le *Cloud Act*[47]. Celles-ci peuvent être particulièrement impactantes dans la mesure où de nombreux fournisseurs de services numériques (réseaux sociaux, hébergement) sont réalisés par des prestataires américains, que cela soit sur leur propre sol ou non.

Le *Patriot Act* est une disposition datant de 2001 permettant aux agences gouvernementales américaines, telles que la CIA ou le Federal Bureau of Investigation (FBI), d'obtenir toute information hébergée sur le sol américain si elles le juge nécessaire dans le cadre d'enquête de lutte contre le terrorisme.

De son côté, le *Cloud Act* permet aux autorités américaines, si elles le justifient par un besoin dans le cadre d'une enquête judiciaire, d'accéder aux données dont une entreprise américaine a le contrôle, en l'occurrence un fournisseur de services d'hébergement, ou *Cloud*. Fait important de cette disposition, c'est la nationalité du fournisseur de services qui fait foi, et non la localisation des données. En d'autres termes, même des données hébergées dans un centre de données sur le sol français seront sujettes à cette loi si l'hébergeur est un acteur américain tel que *Google* ou *Microsoft*. Toutefois, à la différence du *Patriot Act*, le *Cloud Act* nécessite un mandat. Il ne s'agit pas ici d'une enquête secrète comme elle pourrait être menée par une agence gouvernementale.

De manière générale, il faudra toujours veiller dans quelles conditions les lois d'autres pays sont applicables et peuvent faire peser un risque informationnel sur l'entreprise. L'endroit où sont hébergées les données ou l'utilisation de certains outils étrangers peuvent amener à poser une réflexion en ce sens. De manière globale, une stratégie visant à rendre le droit français applicable au maximum aux différents composants de l'environnement de l'entreprise pourra permettre d'avoir une meilleure maîtrise du risque. A défaut, la pleine conscience de ces enjeux s'avère nécessaire pour mettre en place d'éventuelles solutions de contournement (chiffrement des données sensibles hébergées sur un cloud non souverain par exemple).

[47] **Le Mag IT. 2018.** Quelles différences entre CLOUD Act et PATRIOT Act (et quels impacts sur les entreprises françaises). [En ligne] 21 août 2018. [Consulté le 01 avril 2022.] https://www.lemagit.fr/conseil/Quelles-differences-entre-CLOUD-Act-et-PARTIOT-Act-et-quels-impacts-sur-les-entreprises-francaises.

1.7.8. Synthèse opérationnelle : l'investigation numérique

Dans son exposé, l'avocat Eric Barbry souligne les nuances à apporter sur l'investigation en ligne (veille spécifique, OSINT, etc.) et la manière dont cette pratique s'intègre avec les grandes lignes du droit français et européen que nous venons d'énoncer. On parle bien ici « d'investigation », et non « d'enquête », qui par définition est confiée à des autorités (la police ou la CNIL par exemple) ou à des acteurs privés soumis à une législation particulière tels que les détectives privés.

Pour l'expert, n'importe quelle personne est autorisée à mener une investigation, au même titre qu'un journaliste par exemple. Il en va de même pour la réalisation d'études comparatives ou la « rétro-ingénierie » qui ne sont pas des activités proscrites par défaut.

Pour rester conforme au droit, de manière générale, il faut bien discerner le type d'environnement relatif à la donnée qui va être collectée pendant l'investigation. On en distingue quatre distincts :

1. **Privé** : Il s'agit de l'environnement absolument privé de l'entreprise sur lequel est stocké son information. Ici, l'accès aux données n'est pas public la collecte de celles-ci nécessite donc une intrusion dans le système, illicite comme nous l'avons vu

2. **Public** : Les données sont mises à la disposition du public. Elles peuvent être en principe collectées mais peuvent être soumises au droit relatif à la protection des bases de données comme nous l'avons vu, ou encore soumises à la propriété intellectuelle de leur auteur. Il faudra donc juger de ces caractéristiques avant de procéder à la collecte ou l'utilisation de telles données

3. **Données publiées** : Les données ont été publiées sur un environnement restreint mais ne sont pas complètement rendues publique. Par exemple, cela sera le cas si un salarié poste des informations sur son profil professionnel LinkedIn : les données sont publiées auprès de son réseau mais ne sont pas librement accessible par n'importe qui depuis un moteur de recherche par exemple

4. **Informations non publiques mais accessibles** : Il s'agit enfin des données qui sont inaccessibles pour le grand public, mais qui peuvent être accessibles par une manipulation technique simple. Par exemple, il pourra s'agir d'informations contenues sur le code source d'une page web visitée.

Les derniers cas sont plus sujets à interprétation. Il faudra arriver à pondérer son approche entre la protection des données et le besoin d'investigation et se questionner sur l'utilisation des outils pour parvenir à collecter l'information. En d'autres termes, il faut trouver un compromis entre besoin opérationnel et éthique. Spécifiquement, il pourra être utile d'identifier les outils qui sont utilisés et les outils qui sont détournés pour y parvenir. Cette identification pourra servir d'argumentation en cas de litiges entre l'investigateur et le propriétaire des données.

Maître Barbry recommande ainsi « Une veille ou investigation numérique maîtrisée » pour permettre de réaliser les actions nécessaires tout en restant conforme au droit applicable. Il sépare les aspects défensifs et offensifs et fournit une série de recommandations :

- **Aspect offensif (ou « défense active ») : Maîtriser ses actions pour se conformer au droit**
  - Définir des règles claires en matière d'investigation, fixant les limites. En cas de problème, ces règles peuvent être présentées à une juridiction pour plaider la bonne foi et indiquer que ces dernières existent même si elles n'ont pas forcément été suivies
  - Former les équipes en charge de l'investigation à l'outillage qu'ils vont utiliser et les sensibiliser aux limites légales de leurs actions
  - Avant d'investiguer chez un concurrent en cas de soupçon de détournement ou vol de données, une requête pourra être faite auprès d'un juge ou un huissier de justice en amont pour mener un certain nombre de vérifications préalables
  - Utilisation des services d'un prestataire spécialisé ou huissier de justice pour établir les constats de détournement de données. Ces constats seront mieux reçus que de simples captures d'écran effectuées lors de l'investigation

- **Aspect défensif : Protéger son patrimoine informationnel**
  - Déployer les mesures techniques et organisationnelles qui permettront de sécuriser les données de l'entreprise, en particulier les plus sensibles d'entre-elles
  - Définir clairement dans une base contractuelle les conditions d'utilisation d'un site ou d'une plateforme, par exemple en fournissant à ses utilisateurs des Conditions Générales d'Utilisation (CGU)
  - Tracer les données ou créer un périmètre factice de manière à identifier les exfiltrations frauduleuses. Nous entrerons dans le détail de ces stratégies de leurre plus tard dans le document. Éventuellement, ceux-ci pourront faire l'objet d'une validation par un huissier de justice avant d'être mis en place, pour s'assurer qu'ils pourront être recevables par un tribunal le cas échéant

Pour terminer ce chapitre, il est utile de noter que ces recommandations valent pour la législation française, mais qu'il existe de nombreuses jurisprudences en la matière, très variables d'un pays à l'autre. Pour illustrer cette idée, nous pouvons évoquer le cas du réseau social LinkedIn[48], qui a récemment attaqué une entreprise (HiQ) qui collectait les données publiques se trouvant sur les profils publics du réseau. En avril 2022, la cour d'appel californienne a donné raison à HiQ. Il n'a pas été jugé que le fait de collecter des données publiques soit illégal. De plus, le juge a conclu que les données n'appartenaient pas au réseau social et que les utilisateurs s'attendaient de manière évidente que les données soient collectées si celles-ci étaient publiées.

Des jurisprudences françaises en la matière sont de plusieurs ont des interprétations différentes. Par exemple, la Cour de cassation a jugé que des données issues du profil privé d'un employé pouvaient être utilisées par un employeur pour le licencier, dès lors que les informations étaient indispensables pour faire valoir son droit et que leur collecte était « proportionnée » au but poursuivi par l'entreprise

[48]**BOHIC, Clément. 2022.** Scraping : LinkedIn à nouveau freiné dans son combat. *Silicon.* [En ligne] 9 avril 2022. [Consulté le 29 avril 2022.] https://www.silicon.fr/scraping-linkedin-freine-combat-436577.html.

(jurisprudence Petit Bateau, 2020[49]). La jurisprudence Weezevent[50] (2017) quant à elle condamne la collecte de données publique, indiquant que l'utilisation de script de collecte automatisée caractérise l'intention frauduleuse. Des décisions par conséquent très loin du cas LinkedIn précédemment évoqué.

De la même manière que pour les législations elles-mêmes, les jurisprudences doivent être connues et suivies régulièrement, l'environnement juridique évoluant assez rapidement en la matière. Les recommandations doivent donc s'adapter, au cas par cas au contexte de l'investigation menée.

1.7.9. Ce qu'il faut retenir

[49] **Cabinet Soulier Avocats. 2020.** Un post Facebook à ses « amis » peut conduire au licenciement. [En ligne] 30 octobre 2020. [Consulté le 29 avril 2022.] https://www.soulier-avocats.com/un-post-facebook-a-ses-amis-peut-conduire-au-licenciement/.

[50] **LEGALIS. 2017.** Condamnation pour collecte et extraction frauduleuse de données. [En ligne] 7 novembre 2017. [Consulté le 29 avril 2022.] https://www.legalis.net/actualite/condamnation-pour-collecte-et-extraction-frauduleuse-de-donnees/.

1.8. Périmètre de l'étude

Proposer un modèle « clé en main » s'adaptant à n'importe quelle entreprise sur un sujet si vaste que la guerre de l'information n'est pas chose facile. D'une part, parce qu'il existe une multitude de profils d'entreprises pouvant être exposées – ou non – à ce type de risque. D'autres parts, parce que les sujets de l'intelligence économique et de la cybersécurité sont extrêmement vastes.

Le présent chapitre s'attache à proposer un cadrage du sujet qui nous paraît pertinent, à mi-chemin entre ces deux disciplines et pour les entreprises que nous supposons être le plus dans le flou dans la définition de leurs priorités et leur stratégie en la matière.

1.8.1. Les Entreprises de Taille Moyenne (ETI) au cœur de notre cible

D'abord, il nous paraît pertinent d'adresser en priorité ce papier aux Entreprises de Taille intermédiaires (ETI) et non pas forcément aux PME ou aux grands groupes.

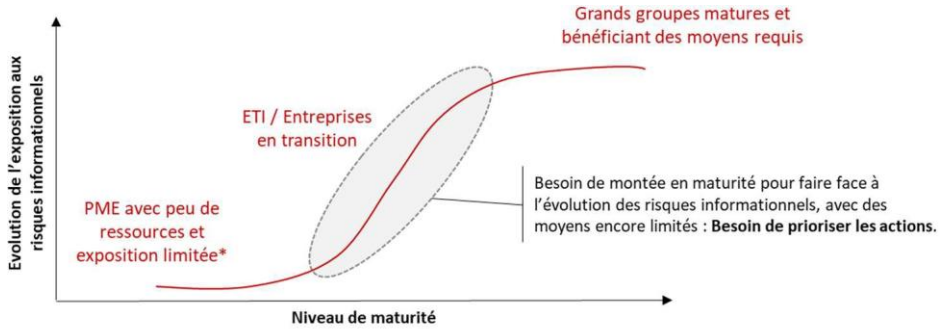
Ensuite, il nous apparaît qu'hormis quelques PME travaillant dans des secteurs particulièrement sensibles ou stratégiques, ces dernières ne sont pas les plus exposées à ce type de risque. De plus, nous estimons qu'avec des ressources limitées, les enjeux liés à la guerre de l'information ne représentent pas un risque suffisamment important pour être pris en compte avant une taille critique.

Les Grands groupes quant à eux, qu'ils soient nationaux ou internationaux, nous paraissent pour la plupart d'entre eux plus mature sur la question. Ils bénéficient déjà des ressources nécessaires pour assurer un premier niveau de traitement des risques. Nous les considérons par conséquent déjà au fait et ne nécessitant pas un guide pratique et « opérationnel », même si ceux-ci pourraient toujours utiliser le modèle afin d'évaluer leur maturité.

Bien sûr, ces arguments ne seront jamais vrais dans la totalité des cas. Le modèle présenté pourra convenir à certaines PME très alertées et / ou exposées, ou des Grands groupes ne jugeant pas encore avoir la maturité suffisante pour faire face à ces risques. Mais ce sont les ETI qui nous semblent les plus intéressantes à cibler. La raison est simple : notre modèle a pour objet de proposer un outil de priorisation et de définition de stratégie. Ainsi, il nous paraît convenir en priorité aux entreprises :

- Encore peu mature sur ces questions pour le grand nombre.
- Bénéficiant de moyens minimaux à investir en la matière.
- Évoluant dans un contexte mouvant où leurs moyens et / ou leur exposition sont variables.

Nous tentons donc de proposer une modélisation flexible capable de couvrir un contexte interne (contraintes, moyens) et externe (exposition aux attaques informationnelles) mouvant.



*Hors secteur stratégiques ou particulièrement sensibles

1.8.2. Un défi majeur dans la limitation du périmètre

Nous l'avons vu dans la première partie, le périmètre de la *Guerre de l'Information* est particulièrement vaste. En déroulant la pelote, nous pourrions facilement couvrir l'ensemble du périmètre lié aux univers de l'intelligence économique et de la cybersécurité, de manière globale.

Pour illustrer cette difficulté, prenons l'exemple tristement courant d'une attaque par rançongiciel. Nous sommes ici clairement dans le domaine de la cybersécurité et les motivations des attaquants sont la plupart du temps lucratives et non informationnelles. Rien à voir avec la Guerre de l'Information donc ? Indirectement, nous y sommes toujours. Pour mettre la pression à leurs victimes, de nombreux groupes de rançongiciels pratiquent la « double-extorsion »[51] et menacent leurs victimes de dévoiler les données compromises au grand public si la rançon n'est pas payée, en plus de les chiffrer. Les données ainsi publiées pourront ainsi mener à une attaque informationnelle opportuniste par une organisation tierce, un concurrent de l'entreprise victime par exemple, qui récupérerait ces informations.

Ainsi, comment définir clairement un périmètre d'actions sur le plan de la Guerre de l'Information, en trouvant le bon compromis et le bon équilibre entre intelligence économique et cybersécurité ? Le défi n'est pas simple. D'ailleurs, et nous le verrons plus tard, la plupart des modèles et guides pratiques pour les entreprises existant sur cette thématique ne nous semblent pas avoir trouvé cet équilibre, penchant soit d'un côté, soit de l'autre. Parce qu'aucun référentiel n'existe à nos yeux pour rapprocher les deux notions.

Il n'existe pas de modèle ou référentiel rapprochant les notions d'intelligence économique et de cybersécurité. Pour trouver l'équilibre et le bon niveau de discours pour définir les actions clés à mener, il faut donc trouver le bon modèle commun.

Selon nous, le référentiel MITRE ATT&CK peut servir de base à ce rapprochement.

Nous allons voir pourquoi.

[51] **Zscaler. 2021.** What Is Double Extortion Ransomware? [En ligne] 2021. [Consulté le 05 mai 2022.] https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware.

Chapitre 2

Le référentiel MITRE ATT&CK

2.1. Un référentiel cyber reconnu

Le *framework* est construit sur une approche empirique. Il référence l'ensemble des techniques utilisées par les acteurs malveillants pour mener des cyberattaques, sur la base de modes opératoires déjà observés et documentés. Il s'articule autour de 14 tactiques, qui sont les objectifs visés par un attaquant lors des différentes phases d'attaque. L'ensemble des tactiques constitue le schéma d'attaque global, en d'autres termes la *cyber kill-chain*.

Les premières phases vont décrire la manière dont les attaquants effectuent une reconnaissance sur leur cible, par l'acquisition d'information par des techniques de scan ou d'investigation en source ouverte (OSINT). D'autres phases vont décrire les moyens pour les attaquants de réaliser un accès initial dans le système d'information ciblé, puis d'exécuter un logiciel malveillant (*malware*), élever leurs privilèges, se latéraliser à l'intérieur du système pour trouver y les équipements intéressants à viser, etc.

Pour chaque tactique, ou étape de l'attaque, on trouve une série de techniques, qui sont les moyens pour un attaquant d'y parvenir. Nous l'avons évoqué, la récolte d'information sur la victime sera utile pour la phase de reconnaissance, la technique de l'hameçonnage est un exemple de technique permettant un accès initial, la force brute pourra servir à voler des identifiants. L'illustration[54] ci-dessous montre un aperçu de cette matrice. En tout, ce sont 191 techniques[55] qui sont répertoriées sur la version 11 du référentiel (avril 2022).

[54] The MITRE Corporation. *Enterprise Matrix*. MITRE ATT&CK [en ligne]. 2022. [Consulté le 02 mai 2022]. Disponible à l'adresse : https://attack.mitre.org/matrices/enterprise/

[55] The MITRE Corporation. *Updates – April 2022*. MITRE ATT&CK [en ligne]. 2022. [Consulté le 02 mai 2022]. Disponible à l'adresse : https://attack.mitre.org/resources/updates/updates-april-2022/

Une des caractéristiques fondamentales du modèle est de fournir pour chaque technique les informations qui permettent de les croiser avec d'autres informations et définir une stratégie de défense. Ainsi, pour chaque technique, seront indiqués :

- Les groupes cybercriminels connus auxquels sont attribuées les attaques utilisant cette technique
- Les sources de données nécessaires à sa détection (ex : évènements de sécurité)
- Les logiciels malveillants pouvant être utilisés pour réaliser celle-ci
- Les mesures d'atténuation, ou « *mitigations* »

Le référentiel MITRE ATT&CK peut ainsi être utilisé à un niveau macro ou stratégique (« Quelle est ma stratégie de détection ? ») mais aussi à un niveau opérationnel (« Quelles sont les mesures techniques à mettre en place pour prévenir ces techniques d'attaque ? »).

Par souci de simplification, nous ne rentrerons pas dans le détail, ni de l'ensemble des tactiques, ni de l'ensemble des techniques, ni de l'ensemble des matrices. Le référentiel compte en effet plusieurs matrices de ce type, adaptées aux différents types d'environnements techniques (Mobile, industriel, etc.).

Nous proposons de nous focaliser sur la tactique « Reconnaissance » qui nous paraît fournir une délimitation idéale au périmètre de cette étude.

2.2. La phase de reconnaissance, au cœur de la guerre de l'information

Nous l'avons vu, de nombreux périmètres du référentiel ATT&CK sont très techniques, et très orientés sur les aspects de cybersécurité. Nous proposons de nous concentrer sur la première tactique, la phase de Reconnaissance, qui regroupe 10 techniques.

Deux éléments notables nous guident dans ce choix de définition du périmètre :

- D'abord, parce que l'ensemble des techniques énoncées dans cette tactique sont d'ordre informationnel, comme l'indique la description globale de la mesure :

Reconnaissance (TA0043)[1]

« *The adversary is trying to* ***gather information*** *they can use to plan future operations.*

Reconnaissance consists of techniques that involve adversaries actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the adversary to aid in other phases of the adversary lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts. »

- Ensuite, parce que certaines des techniques ne peuvent pas être « mitigées » uniquement par une approche Cyber. Une approche externe à l'entreprise, d'ordre informationnel est nécessaire pour faire face. Pour de nombreuses techniques décrites dans la tactique « Reconnaissance », le référentiel lui-même admet que les mesures d'atténuation (sous-entendues techniques) ne peuvent pas être facilement être mises en œuvre :

> *« This technique cannot be easily mitigated with preventive controls since it is based on behaviours performed outside of the scope of enterprise defences and controls. Efforts should focus on minimizing the amount and sensitivity of data available to external parties.»*[1]

C'est ici que nous trouvons le point de convergence entre les deux disciplines. En effet, ce sont des mesures du domaine de l'intelligence économique qui vont venir compléter les mesures techniques de cyberdéfense pour couvrir l'ensemble des méthodes d'attaque.

Nous proposons le **modèle MITRE ATT&CK** sur les aspects défensifs, pour le suivi de la couverture des risques informationnels sur les aspects de reconnaissance, préalables à la mise en œuvre d'une attaque.

Le modèle nous **semble concilier Intelligence Economique et Cybersécurité sur la tactique « Reconnaissance »**. Nous allons ainsi tenter de **lier les mesures** que nous proposons au prochain chapitre, **pour couvrir chacune des techniques** de Reconnaissance.

2.3. Détail des techniques et analyse

Le tableau suivant liste les 10 techniques répertoriées dans la phase de Reconnaissance. Pour chacune d'entre elles, nous avons indiqué la synthèse des mesures de prévention que nous proposons de mettre à disposition des entreprises. Ces dernières seront plus longuement détaillées au chapitre suivant.

RECONNAISSANCE	ID MITRE	Mitigation	Préconisation / prévention	Détails - Justifications
Active scanning				
Active Scanning: Scanning IP Blocks	T1595.001	*Pre-compromise (M1056)*	- Importance de la veille dans la guerre de l'information technologique - Management de la surface d'attaque (ex : CybelAngel) - Management de ses données - Besoins de profils cyber et data-scientists - Déploiement des CSIRT régionaux en France	La maitrise de l'information exposée accessible par OSINT est clé pour prévenir la capacité d'action. Une veille technologique permet une anticipation et une capacité de réaction en cas d'identification de vulnérabilité. La donnée, le nouvel or noir du XXIème siècle, se doit d'être gérée comme le plus important des actifs d'une entreprise. C'est pour cela qu'un management de la donnée doit être mis en place et maintenu. La maîtrise de sa défense va aussi beaucoup compter sur le savoir-faire d'équipes IT dédiées et de l'aide des CSIRT régionaux.
Vulnerability Scanning	T1595.002			
Wordlist Scanning	T1595.003			
Gather Victim Host Information				
Hardware	T1592.001	*Pre-compromise (M1056)*	- Importance de la veille dans la guerre de l'information (veille technologique) - Désinformation opérationnelle (mise en place de pots de miel : HoneyPot et HoneyNet) - Besoins de profils cyber et data-scientists - Déploiement des CSIRT régionaux en France - Management de la surface d'attaque (ex : CybelAngel)	La collecte d'informations sur les hosts et l'infrastructure informatique de l'entreprise peut être limitée par une veille et un réduction de la surface exposée sur internet. Des honey pots peuvent être installés pour induire l'attaquant en erreur sur les technologies utilisées et comprendre les modes opératoires utilisés. La maîtrise de sa défense va aussi beaucoup compter sur le savoir-faire d'équipes IT dédiées et de l'aide des CSIRT régionaux.
Software	T1592.002			
Firmware	T1592.003			
Client Configurations	T1592.004			
Gather Victim Identity Information				
Credentials	T1589.001	*Pre-compromise (M1056)*	- Veille fuite de données sensibles (ex : CybelAngel) - Management de ses données - Formation / sensibilisation des employés à l'ingéniérie sociale - Menace interne (Salariés) - Veille image / réseaux sociaux	La collecte d'informations sur les employés de l'entreprise peut être limitée par une veille et une réduction de la surface exposée sur internet. Une veille sur les réseaux sociaux peut aussi et une sensibilisation des salariés sur les risques liés à la diffusion de leurs informations personnelles.
Email Addresses	T1589.002			
Employee Names	T1589.003			
Gather Victim Network Information				
Domain Properties	T1590.001	*Pre-compromise (M1056)*	- Protection de ses noms de domaine - La désinformation opérationnelle (obfuscation / désinformation par le dépôt de noms domaines)	Des noms de domaines (NDD) peuvent être déposés en prévention du cybersquatting. L'obfuscation peut aussi être utilisée pour induire un concurrent en erreur : dépôt d'un NDD semblant indiquer un prétendu positionnement stratégique à venir.
DNS	T1590.002			
Network Trust Dependencies	T1590.003		- La désinformation opérationnelle (mise en place de pots de miel : HoneyPot et HoneyNet) - Management de la surface d'attaque (ex : CybelAngel)	Pour prévenir l'obtention d'information sur l'infrastructure informatique l'entreprise soit surveiller l'exposition de celle-ci (dont le shadow IT). Une désinformation peut passer par le déploiement d'une infra. factice pour identifier les TTP de l'attaquant.
Network Topology	T1590.004			
IP Addresses	T1590.005			
Network Security Appliances	T1590.006			
Gather Victim Org Information				
Determine Physical Locations	T1591.001	*Pre-compromise (M1056)*	- Management de la surface d'attaque (ex : CybelAngel) - Protection physique	**Défensif** : Une maitrise de la diffusion des informations commerciales est utile est peut être suivie et contrôlée par une démarche d'OSINT

Business Relationships	T1591.002		- Importance de la veille dans la guerre de l'information (veille concurrentielle / commerciale - Veille sectorielle - Menace interne (Tiers)	**Offensif** : une veille / renseignement concurrentiel ou commercial peut permettre à localiser une entreprise dans son environnement (relations, offres, etc.)
Identify Business Tempo	T1591.003			
Identify Roles	T1591.004		- Importance de la veille dans la guerre de l'information (veille concurrentielle / commerciale - Importance de la veille dans la guerre de l'information (veille e-réputation / image (réseaux sociaux professionnels)	
Phishing for Information				
Spearphishing Service	T1598.001	*User training (M1017)*	- Menace interne (Salariés) - Formation / sensibilisation des employés à l'ingéniérie sociale - Déploiement des CSIRT régionaux en France	Les défenses contre le hameçonnage ciblées peuvent passer par des solutions de filtrage mais également par la sensibilisation aux salariés à apprendre à repérer ces approches frauduleuses
Spearphishing Attachment	T1598.002	*Software Configuration (M1054)* *User Training (M1017)*		
Spearphishing Link	T1598.003			
Search Closed Sources				
Threat Intel Vendors	T1597.001	*Pre-compromise (M1056)*	- Importance de la veille dans la guerre de l'information (veille technologique - Cyber-renseignement - Menace interne (Tiers)	La Cyber Threat Intelligence couplée à la veille technologique permet de suivre l'évolution des modes opératoires des attaquants et les vulnérabilités exploitées préalables à la réalisation d'attaques. La menace interne représentée par les tiers ayant accès aux données de l'entreprise doit être adressée.
Purchase Technical Data	T1597.002			
Search Open Technical Databases				
DNS/Passive DNS	T1596.001	*Pre-compromise (M1056)*	- Importance de la veille dans la guerre de l'information (veille image / e-reputation) - Veille fuite de données sur le web (ex : CybelAngel) - Besoins de profils cyber et data-scientists - Management de ses données	Une approche de veille / d'OSINT sur les bases de données publiques est intéressante pour repérer l'information technique publiquement accessible. Les données se doivent d'être protégées par les équipes idoines et des plans d'actions doivent être menés lorsqu'une exposition non contrôlée est détectée.
WHOIS	T1596.002			
Digital Certificates	T1596.003			
CDNs	T1596.004			
Scan Databases	T1596.005			
Search Open Websites/Domains				
Social Media	T1593.001	*Pre-compromise (M1056)*	- Importance de la veille dans la guerre de l'information (veille image / e-reputation) - Veille fuite de données sur le web (ex : CybelAngel)	Une approche de veille / d'OSINT sur les moteurs de recherche et réseaux sociaux est utile pour identifier les informations exposées pubiquement. La notion d'encerclement cognitif doit être étudiée pour optimiser la grille d'analyse relative à la e-reputation.
Search Engines	T1593.002			
Search Victim-Owned Websites	**T1594**	***Pre-compromise (M1056)***	- Management de la surface d'attaque	La gestion de la surface d'attaque ou l'OSINT peut servir à identifier les informations non visibles mais pouvant être collectées via des méthodes techniques simples (ex : scrapping)

Chapitre 3

Concepts et outils à disposition des entreprises

3.1. Distinction entre veille et renseignement

Dans les aspects défensifs et offensifs développés dans les chapitres ci-dessous, les termes veille et renseignement seront utilisés. Nous avons souhaité ici évoquer la différence entre ces deux termes.

En effet, la « veille » est associée dans la littérature au « renseignement », mais il s'agit d'un abus de langage. La veille et le renseignement visent tous deux à recueillir de l'information. Toutefois, la veille (plus accessible financièrement) s'apparente à une collecte passive produisant une synthèse d'informations brutes. Plus spécifiquement, la veille stratégique[56] s'intègre dans les travaux relevant du renseignement classique et de l'Intelligence Économique.

Le renseignement, est le fruit du résultat obtenu soit par :

- L'approche classique du cycle de renseignement (adopté par les services secrets) ;
- La nouvelle approche de l'Intelligence Économique, par l'utilisation des sources ouvertes, aussi dénommé OSINT en anglais (pour *Open Source Intelligence*) ou ROSO en français (Renseignement d'Origine Sources Ouvertes).

Par essence, le renseignement est une information « raffinée » car les informations (issues de types de veille ou d'autres types de collectes) auront fait l'objet de recherches approfondies avec l'usage souvent de techniques numériques avancées, nécessitant aux analystes de bien assimiler les informations obtenues, de faire appel à leurs intuitions, de croiser les sources (pour vérifier l'information blanche et grise) et de discerner les informations justes qui pourront être utilisées en fonction contexte ou de la réglementation.

3.2. Aspects défensifs de la guerre de l'information

Cette partie du mémoire a pour objectif de porter à la connaissance des dirigeants de méthodes (non-exhaustives) employées aujourd'hui dans le cadre d'affrontements économiques entre acteurs.

Avant tout, l'objectif est de sensibiliser et convaincre les dirigeants à appliquer une posture défensive et informative dans leurs entreprises pour éviter qu'elles ne soient impactées dans la compétition économique mondiale et nationale.

Nous l'aborderons ici, au travers des adhérences identifiées entre le référentiel MITRE ATT&CK, matérialisées par les processus et les outils disponibles pour une meilleure maîtrise de l'information.

[56] **BERGERON, Pierette , et al. 2009.** *La gestion stratégique de l'information dans Introduction aux sciences de l'information*. Montréal : Presses de l'Université de Montréal, 2009. p. 235. ISBN : 978-2-7606-2114-5.

3.2.1. L'importance de la veille dans la guerre de l'information

« L'expression d'intelligence économique n'est encore connue que d'initiés et reste singulièrement ambiguë : sans doute parce qu'elle est trop souvent comprise dans son acception anglo-saxonne alors même qu'en France, et c'est bien le paradoxe, elle ne couvre le plus souvent que des méthodes classiques et éprouvées de veille concurrentielle. Voilà l'échec majeur des Français : s'être focalisés sur les moyens et avoir occulté les fins… »[57] *- Extrait du rapport Carayon (2003).*

La documentation relative à la mise en place de la veille stratégique au sein d'une entreprise n'est pas nouvelle et est disponible très largement sur internet depuis plus de 25 ans. Comme l'introduisent tous les manuels de mise en place d'une cellule de veille, ce dispositif permet sans conteste d'être compétitif, concurrentiel et de déployer une stratégie permettant de mieux maîtriser et appréhender l'environnement externe de l'entreprise. Une équipe de veilleurs en mesure de collecter des informations cruciales comme des brevets tombés dans le domaine public ou la publication de travaux de recherches peut constituer des opportunités commerciales et d'innovation.

Cependant, force est de constater que la mise en place d'un tel dispositif est peu considérée par les dirigeants, a fortiori de PME / ETI. Quand bien même la veille stratégique serait-elle considérée comme importante par les dirigeants, cet exercice n'est pas toujours efficace du fait d'une organisation interne non optimisée. Il faut dans un premier temps être conscient que la veille est l'affaire de tous et doit suivre un schéma organisationnel clair (une cellule de veille qui gravite sans rattachement organisationnel fixe ne pourra pas correctement remplir son rôle). Par ailleurs, la veille est une fonction support, qui n'a de sens que si elle répond aux besoins et aux enjeux métier. C'est cette collaboration entre la cellule de veille et le métier qui permettra qu'un plan de veille utile soit mis en place et bénéfique pour l'entreprise.[58]

L'importance d'une veille stratégique doit être reconnue par les domaines publics et privés. Il est impensable que des entreprises fonctionnent au jour le jour sans véritable stratégie de développement, idéalement portée par un organisme de veille faisant office d'aide à la décision. Dans un environnement de guerre économique, maîtriser son apport d'informations fraîches et fiables est devenu indispensable. Grâce à la veille on passe d'une dynamique d'adaptation à une dynamique d'anticipation.[59]

[57] **CARAYON, Bernard. 2003.** Intelligence économique, compétitivité et cohésion sociale. Paris : s.n., 2003.

[58] **Rapport Digimind. 2017.** Les 20 bonnes pratiques essentielles pour votre projet de veille. 2017.

[59] **NANECHE, Matmar. 2018.** La veille stratégique au sein des entreprises modernes. [En ligne] 2018. [Consulté le 17 avril 2022.] https://atlas.irit.fr/PIE/VSST/Actes-VSST2018-Toulouse/Matmar-Naneche.pdf.

3.2.1.1. Les différents niveaux de veille

La veille peut se classer en plusieurs niveaux selon le temps et les ressources que l'entreprise souhaite investir. La mise en place d'une cellule de veille complexe ne se justifie pas forcément, et les dirigeants doivent dans un premier temps définir leurs besoins.

Les dirigeants peuvent commencer par évaluer leur comportement vis-à-vis de la veille[60] :

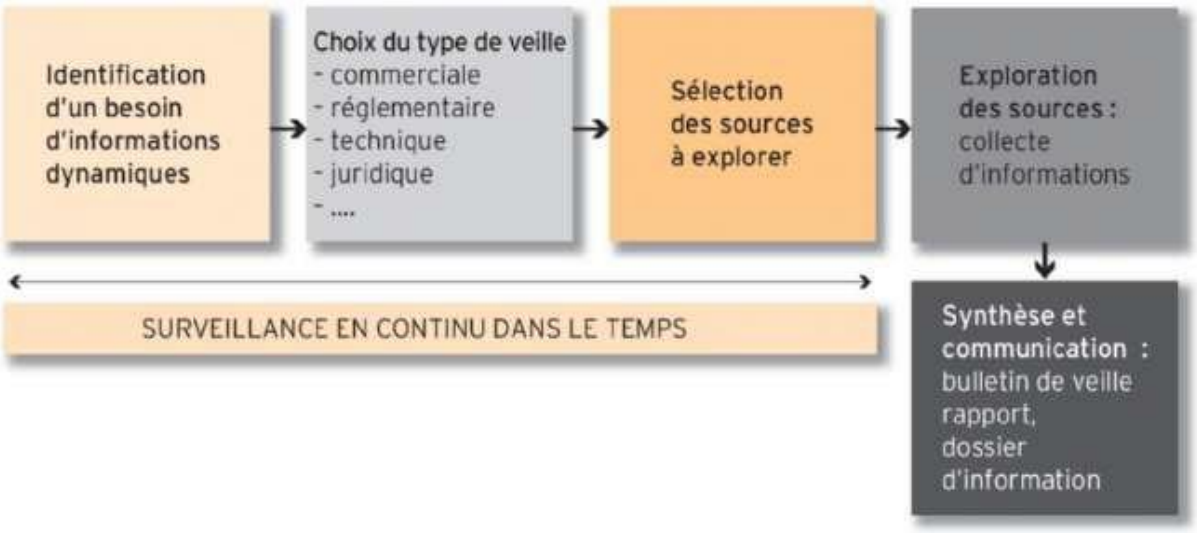
- **Passif** : les décisions stratégiques se font indépendamment de toute analyse informationnelle issue du marché, des concurrents, de l'actualité…
- **Préactif** : les dirigeants s'informent mais n'ont pas mis en place de système pérenne et systématique de collecte d'informations, ce qui leur permet d'éviter des dangers et de s'adapter.
- **Réactif** : l'entreprise a mis en place un système de veille qui lui permet d'éviter les dangers et d'identifier des opportunités.
- **Proactif** : l'entreprise a complètement inclut la veille dans son processus décisionnel, jusqu'à tenter d'influencer le marché et d'agir sur son environnement.

Ensuite, il est possible de distinguer le type de veille désiré pour faire évoluer son comportement. Nous pouvons distinguer :

- **La veille ponctuelle :** c'est le premier niveau de veille, qui répond à un besoin d'informations très spécifique et s'attache à décrire une situation à un moment donné. La recherche est réalisée de manière ad hoc, sur un sujet précis et sur une durée définie. Elle peut être mise en place lors d'une période de crise, afin d'obtenir les données nécessaires à sa résolution.
- **La veille occasionnelle** : la direction a ciblé un sujet à surveiller et a adapté son organisation afin de collecter des informations de manière plus régulière. La veille occasionnelle peut venir compléter une veille ponctuelle afin de l'actualiser, l'approfondir, ou challenger les précédentes recherches réalisées sur ce même sujet.
- **La veille périodique :** cette veille est utilisée comme une aide à la décision car il est possible de dégager une tendance suite à l'analyse des données collectées. La surveillance régulière de la cible va inclure un plus grand nombre de paramètres (temporels, géographiques, types d'acteurs, types de sources d'information…).
- **La veille permanente :** elle n'est possible que lorsqu'une cellule et des ressources dédiées sont mises en place par l'entreprise. La veille permanente vise à capter l'ensemble des informations relatives à l'environnement ciblé. Elle permet véritablement à l'entreprise d'être pro-active vis-à-vis du marché et de sa stratégie.

[60] **CHAABEN, Mariem et FOUGHALI, Wafa. 2017.** La cellule de veille au sein du CTAA (Centre Technique de l'agro-alimentaire). [En ligne] 23 mars 2017. [Consulté le 27 avril 2022.] https://fr.slideshare.net/mariemchaaben/etude-decascelluledeveille.

La veille apportera un avantage concurrentiel concret à condition que sa mise en place suive les 5 étapes clés suivantes :



Les 5 étapes clés de la veille[61]

3.2.1.2. Les différents types d'information[62]

Collecter et stocker des informations dans le cadre de sa veille ne suffit pas. Il faut catégoriser le type de données afin d'adapter son système de veille et éviter tout risque légal. Il faut différencier les types d'informations existants :

- **Information blanche :** il s'agit de la majorité des données utiles à l'entreprise. En effet, le recours à l'OSINT est permet d'obtenir toutes les données accessibles en source ouverte, formelle ou officielle. Elle est par définition en accès libre (que ce soit voulu ou non). Le principal défi est de faire le tri dans la masse gigantesque de données accessibles : sites institutionnels, sites d'entreprises, travaux de recherches, baromètres, données publiées sur les réseaux sociaux…

- **Information grise :** plus difficile d'accès, ce type d'information reste licitement accessible. Elle peut être éphémère ou informelle.

- **Information noire :** il s'agit sans aucun doute du type de donnée qui permettra aux entreprises d'avoir un avantage concurrentiel du fait de son caractère confidentiel et/ou critique. Son obtention peut être frauduleuse ou due à une mauvaise sécurisation des données par l'entité détentrice de cette information. De plus, l'information noire peut être d'origine humaine, récoltée via un échange avec un client, un partenaire, un fournisseur, lors d'une conférence ou même par de l'ingénierie sociale (illégal).

[61] **BENOIT-CERVANTES, Géraldine. 2017.** La veille sur Internet. [En ligne] 30 novembre 2017. [Consulté le 27 avril 2022.] https://www.e-marketing.fr/Thematique/academie-1078/fiche-outils-10154/La-veille-sur-Internet-324957.htm#.

[62] **GLOAGUEN, Philippe.** Le guide l'intelligence économique. Le Routard. [en ligne]. 1° édition. Italie : HACHETTE LIVRE 2014. 143 pages. ISBN-301-00-00-03-62-96 [consulté le 12 mai 2022]. Disponible à l'adresse : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/routard-guide-intelligence-economique.pdf

3.2.1.3. Les domaines de la veille

Le pivot qui impactera tout ou presque une stratégie de veille est le domaine dans lequel l'entreprise souhaite investir du temps et des ressources. Ce travail de circonscription a pour objectif de définir l'environnement à surveiller, encore une fois selon l'objectif retenu. Faut-il faire une veille scientifique et technique pour de la Recherche & Développement, ou juridique pour une fusion / acquisition, ou encore concurrentielle et commerciale pour tenir ses concurrents à l'écart[63].

Non seulement, le domaine de veille fera varier les modes opératoires de recherche, mais aussi les ressources humaines qui interviendront et qui se devront d'être expertes dans ce domaine. Voici une cartographie des principaux types de veille, exposant la finalité générale, les objectifs précis et les moyens de chacun d'entre eux[64].

[63] **BELIMANE, Wissam et RHANI, Amel. 2010.** La mise en place d'un système de veille commerciale. [En ligne] 2010. [Citation : 26 avril 2022.] https://www.memoireonline.com/12/11/4977/m_La-mise-en-place-dun-systeme-de-veille-commerciale5.html.

[64] **GEROUDET, Marie-Madeleine. 2013.** Types de veilles. [En ligne] 2013. [Consulté le 28 avril 2022.] http://www.ressources.univ-rennes2.fr/cultures-numeriques-dans-l-enseignement/veille/1-quest-ce-que-la-veille/types-de-veilles/.

	Veille image	Veille réglementaire, normative et juridique	Veille technologique / innovation	Veille sectorielle / stratégique	Veille commerciale	Veille concurrentielle	Veille financière
Pourquoi ?	Evaluer votre image et votre réputation sur le net	S'informer des évolutions réglementaires de votre marché	Appréhender les évolutions et les innovations de votre marché	Connaître et anticiper les évolutions de votre marché	Détecter les nouvelles opportunités	Connaître vos concurrents sur le bout des doigts	Évaluer la santé financière de votre environnement (partenaires, fournisseurs, concurrents) et de votre marché
Comment ?	Cartographier les relais d'influence et suivre la propagation d'un message	Surveiller la presse et les sites d'information spécialisés	Surveiller la presse et les sites d'information spécialisés	Surveiller l'actualité sur le web, dans la presse locale, nationale et spécialisée	Identifier une cible précise (chiffre d'affaires, nombre de salariés, zone géographique) et surveiller les signaux faibles dans la presse, sur internet et sur le terrain	S'informer sur leurs prestations, leurs produits, leurs prix, leurs clients…	Surveiller la presse spécialisée et les sites d'information d'entreprise
	Surveiller l'actualité qui vous concerne dans la presse écrite, TV, radio	S'informer des débats parlementaires, projets de lois en cours, des propositions gouvernementales et syndicales	Surveiller les dépôts de marque, dessins ou modèle, et brevets qui concernent votre marché	S'informer sur les tendances comportementales et sociétales		Surveiller l'actualité de vos concurrents sur le web, dans la presse locale, nationale et spécialisée.	
	Surveiller les réseaux sociaux et espaces de discussion en ligne	Surveiller les procédures judiciaires en cours et les nouvelles jurisprudences	Rechercher les nouvelles publications et travaux de recherche	Participer aux associations et aux syndicats professionnels	Surveiller les appels d'offre sur internet et dans la presse spécialisée	A coupler avec les veilles financière et technologique	Surveiller les cours en bourse des entreprises et des matières premières qui vous concernent
			S'assurer du respect de vos droits à la propriété intellectuelle	Participer aux salons et rendez-vous de votre secteur			
Objectifs	Savoir que qu'il se dit de vous dans les médias et comment	Être à jour quant aux normes et règlementation en vigueur	Anticiper les mutations technologiques de votre marché et connaître les mouvements de vos concurrents	Identifier les menaces et opportunités, les leviers de croissance ou à l'inverse les activités en perte de vitesse	Développer votre potentiel commercial	Connaître les mouvements de vos concurrents (recrutements, acquisitions, nouvelle marque…)	Être informé des dangers potentiels (mauvais payeur par exemple) et inversement d'opportunité
	Anticiper une situation de crise	Anticiper les changements à venir et vous adapter	Protéger votre patrimoine immatériel, notamment technologique		A partir de nouvelles sources d'information, identifier de nouveaux clients, fournisseurs, partenaires…	Évaluer leur positionnement et le comparer au vôtre	Identifier les mouvements de vos concurrents (fusion, acquisition)
	Utiliser ces informations pour adapter vos produits et innover						Comparer votre santé financière à celle de vos concurrents
Vers qui se tourner ?	Experts en communication et en « e-réputation » … Conseils en propriété intellectuelle (dessins, modèles…)	Pouvoirs publics, organismes de normalisation, avocats, experts-comptables, organismes de gestion agréés, notaires…	INPI, ARIST, réseau des conseillers et attachés scientifiques et techniques des ambassades de France, pôles de compétitivité, AFNOR…	Pouvoirs publics, ONG, conseils en stratégie…	Chambres de commerce et d'industrie, Chambres de métiers et de l'artisanat, organisations professionnelles, Ubifrance…	Chambres de commerce et d'industrie, Chambres de métiers et de l'artisanat, organisations professionnelles, Ubifrance…	Experts-comptables, commissaires aux comptes, organismes de gestion agréés, Autorité des marchés financiers (AMF)…

3.2.1.4. Structure organisée dans l'entreprise : la cellule de veille

La mise en place d'une cellule de veille au sein d'une organisation se construit et se pense dans la durée. Pour maximiser les chances que la cellule de veille soit efficace et que le fruit de son travail soit pleinement intégré dans les décisions stratégiques, il convient de réfléchir sur la raison d'une telle mise en place, mais aussi du type d'intervenant et de la communication (entre les parties prenantes et à destination du top management). La cellule de veille a-t-elle vocation à capter de l'information réglementaire, concurrentielle, financière, commerciale ? Comme décrit dans le tableau précédent, la source de l'information, les leviers disponibles, les manières de capter l'information ou encore les parties prenantes diffèrent grandement selon l'objectif visé.

Il faut aussi prendre conscience que la veille n'est pas uniquement le rôle des veilleurs. En effet, il serait contre-productif de négliger les veilleurs informels et les veilleurs potentiels. [65] Cela nécessite donc d'élargir le champ des possibles en mettant en place une culture de la remontée d'information.

Catégorie de veilleurs	Détails et interactions	Description
Veilleurs formels	Les veilleurs à temps plein : interactions directes avec les décideurs	Ce sont les veilleurs de la cellule de veille centrale de l'entreprise. La veille correspond à 100% de leur travail. Ce sont des veilleurs formels au sens où ils sont reconnus comme tels par le management et évalué sur leurs activités de veille.
	Les veilleurs à temps partiel: interactions directes avec les décideurs	Les acteurs font de la veille de manière formelle au sens où ils sont évalués par leurs supérieurs en partie sur ces activités-là. La veille représente en moyenne entre 25 et 50% de leur activité professionnelle.
Veilleurs informels	Interactions indirectes avec les décideurs	Ces acteurs font partie du réseau de veille informel au sens où ils font de la veille, sont en relation avec les veilleurs formels mais ne sont pas « contraints » ou sollicités officiellement par leur management pour participer au système de veille.
Veilleurs potentiels	Interactions indirectes avec les décideurs	Ce sont des acteurs qui font de la veille sans être en contact avec le système de veille formel/veilleurs formels de l'entreprise.

Catégories de veilleurs [66]

Avantages de l'internalisation :

- Maîtrise de ses connaissances : Ia protection de ses données collectées est primordiale. Le risque de fuites des données à cause d'une cellule de veille externalisée est accru, surtout si l'entreprise ne s'enquiert pas du niveau de maturité Information Technology (IT) de son prestataire. Idem pour une cellule de veille faisant héberger ses données chez un hébergeur.

- Possibilité de personnaliser sa veille pour répondre à ses besoins / connaissance de son marché et de l'entreprise : l'objectif impératif d'une cellule de veille est et reste l'acquisition d'un avantage stratégique grâce à la récolte et l'analyse d'informations. En interne, la définition et la mise en

[65] **Université de Rennes 2.** Définitions de la veille. [En ligne] [Consulté le 28 avril 2022.] http://www.ressources.univ-rennes2.fr/cultures-numeriques-dans-l-enseignement/veille/1-quest-ce-que-la-veille/1-1-definitions-de-la-veille/.

[66] **GUECHTOULI, Manelle et BOUDRANDI, Stéphane. 2013.** Comment se « fabrique » la décision stratégique : le cas d'une cellule de veille stratégique. *CAIRN.INFO.* [En ligne] 01 novembre 2013. [Consulté le 27 avril 2022.] https://www.cairn.info/revue-recherches-en-sciences-de-gestion-2012-1-page-35.htm.

place d'une telle stratégie peut être plus facilement être adaptée selon le besoin, surtout en cas de changement de la stratégie de l'entreprise. À tout moment, il est possible de changer de fusil d'épaule pour conserver sa dynamique.

Inconvénients de l'internalisation :

- Besoin d'adhésion de l'ensemble des parties prenantes : Comme n'importe quel projet informatique, l'important est d'identifier au plus tôt un sponsor qui portera la démarche de mise en place de la veille.[67] Une fois la structure en place, il faut s'attacher à pérenniser le processus et le faire entrer dans la culture d'entreprise, surtout dans un environnement français qui n'est pas habitué à ce mode opératoire. Pour cela, le faire savoir est aussi important que le savoir-faire. Avoir des SPOC (Single Point Of Contact) dans tous les départements ainsi que la mise en place d'une facturation à chaque fois que les services de la cellule de veille sont utilisés peuvent être un moyen de responsabiliser les salariés. Sans adhésion, le projet est voué à l'échec.

- Coûteux : La mise en place d'une veille internalisée est bien évidemment plus onéreuse qu'un service de prestation. En effet, il faut prévoir tous les investissements nécessaires au niveau organisationnel, humain (spécialistes de veille, spécialistes juridiques, data-scientists…) et outils (outil de veille, licences spécialisées pour l'accès à certaines données, outil de reporting, infrastructure dédiée). Le calcul de retour sur investissement doit impérativement être réalisé avant tout lancement d'une cellule de veille.

3.2.1.5. Structure organisée hors de l'entreprise : la veille externalisée

Une fois n'est pas coutume, il peut être plus intéressant pour une entreprise d'externaliser le service de veille. [68] A l'instar de l'hébergement de ses données ou des services d'entretiens, avoir recours à la prestation peut permettre à une entreprise de se concentrer son cœur de métier sans créer de poste en interne. Tout est question de retour sur investissement et de politique interne de l'entreprise.[69] Bien entendu, l'appel à une équipe de veille externe peut venir en complément d'une structure organisée en interne (pour des sujets ponctuels ou relatifs à un domaine non maîtrisé en interne).

Avantages de l'externalisation :

- Flexibilité et maîtrise des coûts : la principale raison d'un manque de veille au sein d'une entreprise vient du fait que la direction ne va pas être encline à investir des ressources humaines et matérielles. Soit le veilleur n'a pas la matière pour travailler à plein temps et serait considéré comme une charge vis-à-vis de la valeur ajoutée, soit l'exercice de veille est attribué à tous les collaborateurs, ce qui constituerait un enjeu organisationnel important pour qu'elle soit efficace.

- Gain de temps : À condition que l'expression de besoin et l'objectif soient correctement réalisés, l'externalisation peut apporter un gain de temps significatif. Le métier bénéficiera de l'information, synthétique, fiable et fraîche à la demande sans perdre de temps à sonder la multiplicité des informations disponibles en source ouverte ou fermée.

---

[67] **MARQUANT, Arnaud. 2022.** Mise en place d'une cellule de veille au sein de l'entreprise : trois actions à consolider. *Global Security Mag*. [En ligne] février 2022. [Consulté le 29 avril 2022.] https://www.globalsecuritymag.fr/Mise-en-place-d-une-cellule-de,20220222,122305.html.

[68] **Vegenov. 2017.** Externaliser sa veille : une solution aux multiples avantages. *Vegenov*. [En ligne] juin 2017. [Consulté le 29 avril 2022.] https://blog.vegenov.com/2017/06/externaliser-veille-solution-aux-multiples-avantages/.

[69] **Inevidence. 2007.** *De l'utilité ou de la nécessité d'externaliser toute ou partie de la veille.* [Présentation Powerpoint] Rabat : s.n., 24 et 25 mai 2007. Séminaire « Veille et Text-Mining ».

- Apport d'expertise extérieure : les prestataires de veille disposent d'une expérience et de bases de données que des analystes internes peuvent prendre des années à développer. De plus, la veille de base sur la recherche de sources ouvertes et / ou fermées, issues d'outils professionnels payants.

Inconvénients de l'externalisation :

- Confidentialité des données : L'exemple de confier l'hébergement de ses données à un prestataire spécialisé s'applique bien au cas de la veille stratégique. En effet, externaliser un processus clé d'aide à la décision inclut des risques quant à la confidentialité des données et des informations recueillies. Il faudra alors s'assurer de la réputation du prestataire (via des certifications reconnues notamment) et de l'existence des clauses de confidentialité dans le contrat et de son niveau de maîtrise de la sécurité. (Se référer au chapitre sur la menace interne pour de détails).

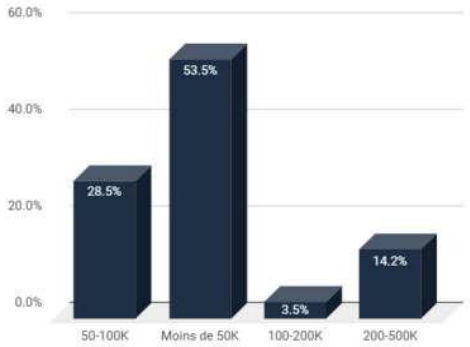
- Compréhension du domaine d'activité : Qu'il s'agisse de la mise en place d'une cellule de veille interne ou externe, l'important reste d'être clair sur l'objectif à atteindre. Ainsi les phases de cadrage peuvent-elle être chronophages, mais nécessaires au risque que les données fournies par le prestataire ne soient pas utilisables par le métier et la direction. Par ailleurs, si le sujet est très pointu, il peut être nécessaire de faire appel à un autre prestataire moins généraliste, plus expert sur le domaine d'intérêt.

3.2.1.6. Tendance « Veille et Market Intelligence » en 2021

Digimind, éditeur de solution de veille et d'analyse des médias sociaux, en collaboration avec Orange Consulting, ont publié en 2021 un baromètre intitulé « État de l'art & tendances Veille et Market Intelligence »[70].

L'étude a été menée auprès de 110 entreprises disposant d'un dispositif de veille, dont 59% employant plus de 500 salariés. Le baromètre conclue que « très peu de TPE & de PME ont les ressources humaines et financières nécessaires pour avoir une fonction dédiée au market intelligence. Les missions de veille sont alors souvent disséminées au sein d'autres postes. »

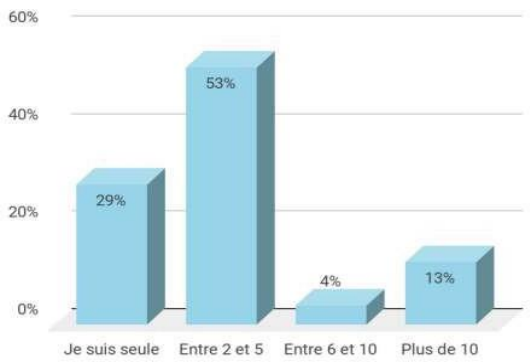
Les budgets des répondants sont majoritairement inférieurs à 100 k€ et en baisse par rapport aux années précédentes (d'après les précédents baromètres Digimind).



Budget alloué à la veille (en €) pour les 110 participants en 2021

[70] **Digimind et Orange Consulting. 2021.** *État de l'art & Tendance Veille et Market Intelligence.* 2021.

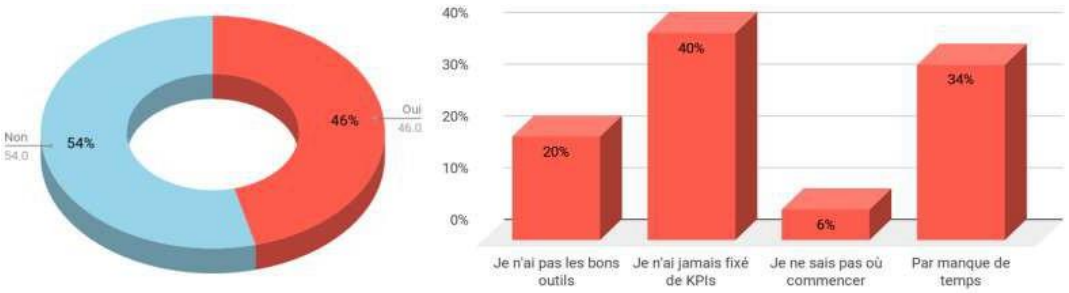
Autre critère mis en lumière par le baromètre, la dimension relativement faible des équipes de veille : 53% des répondants disposent de 2 à 5 salariés dédiés à cet exercice et 29% n'ont qu'un poste dédié.



Dimension des équipes travaillant dans une cellule de veille pour les 110 participants

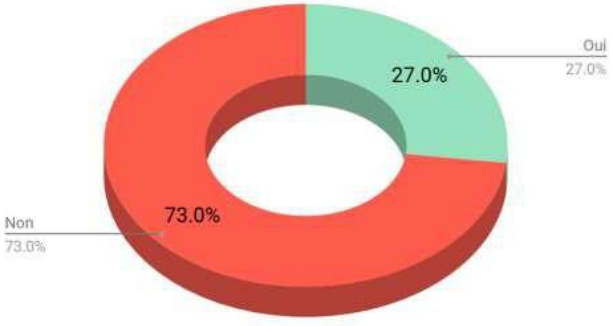
Cela étant dit, intéressons-nous aux principaux constats identifiés par l'étude :

- **Mesure des résultats de la veille** : avec surprise, le rapport montre que 54% des répondants ne mesurent pas leurs Key Performance Indicator (KPI) ou Indicateur clé de performance (ICP) en Français, dont 40% n'en ayant même pas défini. Il est donc impossible de savoir si sa cellule remplit les objectifs visés (de recherche d'avantage concurrentiel) et de ce fait d'adapter sa stratégie si besoin (perte d'agilité et de réactivité).



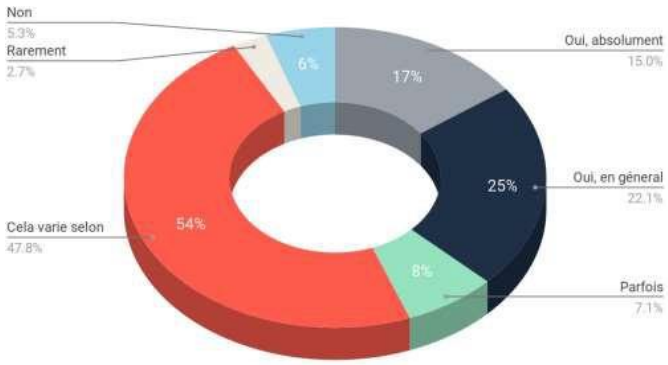
Part des répondants mesurant les résultats de la veille et raisons pour lesquelles les résultats ne sont pas mesurés

- **Reporting** : seules 27 % des directions exigent un reporting sur la performance de la veille. Les cellules de veille agissant proactivement dans la présentation des résultats de la veille à leur direction le font surtout dans le but d'augmenter leur budget et d'obtenir des ressources supplémentaires. Encore une fois, le manque de reporting et de suivi des effets de la veille ne peuvent que défavoriser l'entreprise dans l'établissement de sa stratégie et de son aide à la décision.

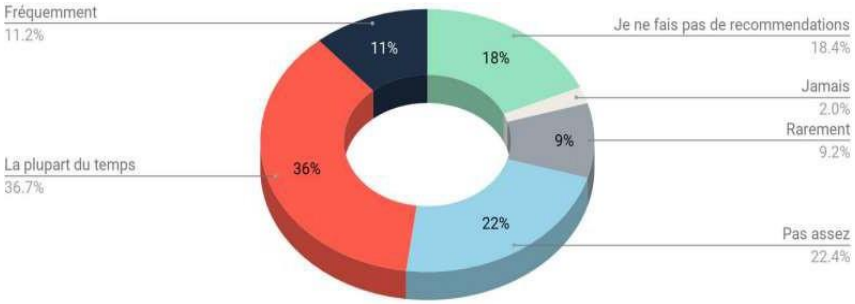


Part des répondants mesurant réalisant un reporting à leur direction

- **Perception de l'impact de la cellule de veille dans la prise de décision** : bien que 16% uniquement des répondants ne se sentent pas leur expertise suffisamment considérée par l'organisation, seul 48% d'entre eux pensent que leurs recommandations sont prises en compte dans le processus de décision (18% ne font même jamais de recommandations).



Part des répondants considérant que l'organisation reconnaît la valeur ajoutée et l'expertise apportée par la cellule de veille



Part des répondants considérant que les recommandations / analyses sont intégrées dans la prise de décisions stratégiques

Les tendances décrites par cette analyse font directement écho au constat du Rapport Carayon, qui date pourtant de 2003 :

- La veille stratégique n'est accessible qu'à une faible part d'initiés.
- Elle est utilisée dans sa forme classique et éprouvée.
- Les entreprises se concentrent plus sur les moyens que sur la fin.

3.2.2. Paradoxe de l'importance négligée de la donnée

« Faire vivre la donnée, c'est dynamiser son business, c'est rendre sa société plus vivable pour ses collaborateurs. Protéger sa donnée, c'est faire survivre son business. »[71] - Philippe Trouchaud - Chief Technology & Products Officer chez PwC France et Maghreb

De nombreux PDG s'accordent à dire que la donnée est un actif indispensable pour le fonctionnement et la survie d'une entreprise, au point d'être la cible principale des attaquants. Si l'avantage concurrentiel issu d'une utilisation judicieuse de la donnée ne fait aucun doute, il peut être très difficile de l'exploiter de manière optimale, et cela pour plusieurs raisons.

3.2.2.1. Des données non organisées

Face à l'ampleur des données accessibles et collectables par les entreprises, leur exploitation peut être difficile. Pire encore, les métiers peuvent avoir tendance à douter de leur fiabilité ou de leur utilité, à moins de passer un certain temps à les traiter et les analyser.[72]

D'après une étude réalisée par Forrester pour Dell Technologie[73], nous apprenons que :

- 61% des équipes Data se sentent débordées par la masse d'information qu'ils ont à traiter, mais pourtant, elles en ont toujours besoin de plus.
- 64% des décideurs affirment qu'ils ont trop de données en leur possession pour pouvoir appliquer une stratégie de sécurisation efficace qui réponde aux exigences basiques de sécurité.
- 70% estiment que les données sont recueillies trop vite pour qu'elles puissent être toutes analysées et utilisées.

Cela met donc en évidence le fait que les entreprises agissent sur un champ trop large et en souhaitant obtenir trop d'informations, aucune n'est réellement exploitable.

La donnée est principalement non-structurée, c'est ce que met en exergue une étude réalisée par MongoDB[74], un éditeur de système de gestion de base de données. Les données non structurées sont des informations qui ne sont pas organisées selon un modèle ou schéma de données prédéfini et ne peuvent donc pas être stockées dans une base de données relationnelle. Il s'agit d'informations générées par des humains (email, photographies, fichiers textes, enregistrements vocaux, logs, messages instantanés…) ou des machines (enregistrements sismiques, données météorologiques, photographies / vidéos de surveillance…). Face à tant de contenu, le défi est de savoir quel type d'information est réellement utile au bon fonctionnement de son activité afin de le prioriser.

---

[71] **TROUCHAUD, Philippe. 2016.** *La cybersécurité au-delà de la technologie*. Paris : Odile Jacob, 2016. pp. 42-43. IBSN : 978-2-7381-3368-7.

[72] **GARO, Jean-Denis. 2021.** Le paradoxe de la charge des données. *La Tribune*. [En ligne] 08 septembre 2021. [Consulté le 25 avril 2022.] https://www.latribune.fr/opinions/tribunes/le-paradoxe-de-la-charge-des-donnees-891771.html.

[73] **Forrester. mai 2021.** *Businesses Must Better Balance Culture And Technology To Improve Data Readiness*. mai 2021. Étude commandée par Dell Technologies.

[74] **MongoDB. 2021.** Unstructured Data. *MongoDB*. [En ligne] 2021. [Consulté le 28 avril 2022.] https://www.mongodb.com/unstructured-data.

On note donc un besoin crucial de cartographier et classer ses données (internes et externes) selon le niveau de criticité, le type et l'utilisation qu'on en fait. [75] En effet, et nous le verrons plus tard, la sécurisation des données va dépendre de sa classification : publique, interne, confidentielle, très confidentielle / restreinte.[76]

La manière dont il est recommandé d'organiser ses données est aussi très largement documentée sur internet et par des experts data et sécurité. Mais là encore, les entreprises ne semblent pas considérer ce sujet comme prioritaire ou semblent démunies face aux difficultés d'une telle mise en place.

3.2.2.2. Un manque de gouvernance de la donnée

Une autre raison plus difficile à admettre par les entreprises est le manque d'ownership de la donnée. En effet, il est fréquent que personne ne sache où les données se trouvent exactement, ou pire encore, qui en est responsable. Rappelons-le : choisir sciemment de ne pas utiliser la donnée relève d'une faute stratégique, constituant un risque sur la survie de l'entreprise[77].

En l'absence d'un Délégué à la Protection des Données (DPO), d'un Chief Data Officer (CDO) ou d'un Data Architect, il est fréquent de constater que les fonctions métiers ne se sentent pas concernés par la gestion de la donnée, à savoir comment elle est maintenue, protégée, diffusée et stockée. Cette tâche est d'ailleurs souvent et injustement déléguée au service informatique. Ce que les métiers ont tendance à oublier, c'est qu'ils sont directement propriétaires de ces données, et qu'il leur revient de les protéger dans l'intérêt de l'entreprise.

D'autre part, il est étonnant que l'actif surpuissant que constitue la donnée soit aujourd'hui géré en silos (60% des répondants de l'étude Forrester considère que les silos constituent un obstacle à la bonne utilisation de la donnée), sans que personne n'en ait une vision globale.

3.2.2.3. Les principales règles de bonne gestion d'une donnée

A la lumière de ce que nous avons appris, nous pouvons dégager plusieurs tendances quant à la gestion de la donnée :

- Admettre que la donnée à un cycle de vie. Il est dangereux de conserver des données obsolètes et en trop grande quantité. Chaque donnée se doit d'être protéger, donc ne conserver que les données utiles permet de réduire la surface d'exposition.[78]

[75] **Converteo. 2017.** 10 critères RGPD pour évaluer vos bases de données. *Converteo*. [En ligne] 11 octobre 2017. [Consulté le 28 avril 2022.] https://converteo.com/blog/10-criteres-rgpd-pour-evaluer-vos-bases-de-donnees/.

[76] **LUSSAN, Pierre-Louis. 2022**. Comment élaborer une politique efficace de classification des données pour une meilleure sécurité de l'information. Netwrix. [En ligne] 13 janvier 2022. [Consulté le 2022 avril 30.] https://blog.netwrix.fr/2018/06/20/comment-elaborer-une-politique-efficace-de-classification-des-donnees-pour-une-meilleure-securite-de-linformation/.

[77] **TROUCHAUD, Philippe. 2016.** *La cybersécurité au-delà de la technologie*. Paris : Odile Jacob, 2016. pp. 42-43. ISBN : 978-2-7381-3368-7

[78] **CNRS. 2014.** Le cycle de vie des données. *inist*. [En ligne] Institut de l'Information Scientifique et Technique, 16 septembre 2014. [Consulté le 30 avril 2022.] https://www.inist.fr/wp-content/uploads/donnees/co/module_Donnees_recherche_7.html#:~:text=D%C3%A9finition,des%20donn%C3%A9es%20de%20la%20recherche..

- Identifier ses actifs informationnels les plus critiques. Certaines informations sont restreintes, d'autres confidentielles (ex : rapports de commissaire aux comptes, données d'acquisitions, propriété intellectuelles, données personnelles…).
- Adopter une gouvernance claire et définir les responsabilités de chacun au sein de l'entreprise. Lorsque les rôles relatifs à la production, l'utilisation et la protection de l'information sont clairs, s'assurer que les bonnes pratiques sont suivies de manière systématique et disciplinée dans le temps.
- Être extrêmement vigilant sur les données qui sont confiées au tiers (fournisseurs, client, partenaires, fournisseurs). Les tiers sont cibles d'attaques qu'il ne faut pas négliger, et une politique adéquate en interne peut être mise en péril par un prestataire ne disposant pas d'un niveau équivalent de sécurité. Cette partie sera détaillée dans la suite de ce document.
- Mener une évaluation périodique de son exposition sur le net. Cela peut passer par une analyse approfondie réalisée par un prestataire spécialisé, ou l'intégration ce volet dans son système de veille (ex : rechercher si des documents internes estampillés « confidentiels » sont accessible en source ouverte, faire des recherches sur les réseaux sociaux et internet afin d'apprendre ce qui en ressort, savoir si sa société est mentionnée sur le darknet…).

3.2.3. La menace interne

« Nous avons découvert au cours de nos recherches que les menaces internes ne sont pas considérées aussi sérieusement que les menaces externes, comme une cyberattaque. Mais lorsque les entreprises avaient une menace interne, en général, elles étaient beaucoup plus coûteuses que les incidents externes. C'était en grande partie parce que l'initié qui est intelligent a les compétences nécessaires pour cacher le crime, pendant des mois, des années, parfois pour toujours. » — Dr. Larry Ponemon, Président et fondateur du Ponemon Institute, think tank dédié à l'avancement des pratiques en matière de confidentialité, de protection des données et de sécurité de l'information.

3.2.3.1. Les salariés

Il est possible d'établir deux schémas distincts de menace interne liée aux salariés.

a. Les salariés négligents

La perte d'un PC non chiffré, une clé USB comportant des données sensibles, une fuite de mot de passe… Bien que cela constitue une faute professionnelle, il n'y a pas d'intention de nuire. Pourtant, cela peut engendrer des risques importants. Pour cela, la meilleure solution est de sensibiliser et former ses salariés. Un chapitre est consacré à ce sujet d'importance critique pour les entreprises.

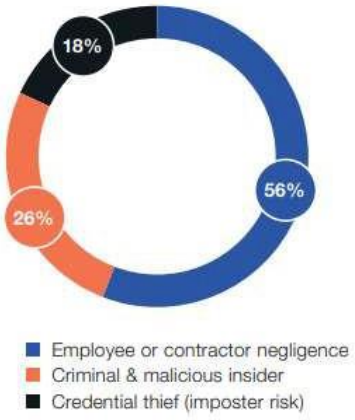
Une étude menée en 2021 par l'entreprise de Cybersécurité Code42, en partenariat avec Aberdeen Strategy & Research[79] ont montré que :

- 33% des fuites de données sont du fait d'un interne.
- 78 % de ces fuites de données internes impliquent une perte ou une exposition involontaire de données, ce qui démontre que le vol et l'exposition malveillante de données ne constituent pas le risque interne le plus important auquel les équipes de sécurité sont confrontées.
- Les fuites de données venant d'un interne coûtent en moyenne 20% du revenu annuel des entreprises participant à l'étude.

Les entreprises ont du mal à maintenir un niveau satisfaisant de sécurité des données, car la plupart d'entre elles ne disposent pas d'une vision cohérente et centralisée sur leurs propres environnements numériques. 75 % des organisations participant à l'étude ne disposent pas des outils nécessaires pour suivre le nombre de mouvements de fichiers au sein de leur organisation et pour surveiller la fréquence à laquelle des fichiers sont exposés par des utilisateurs légitimes effectuant leurs tâches quotidiennes. Les fuites de données sont 4,5 fois plus fréquentes sur un terminal (endpoint) que sur un serveur. Cela concerne notamment les ordinateurs fixes et portables, les téléphones mobiles, les tablettes, les terminaux IoT, les appareils photos…

L'approche idéale pour protéger la donnée d'entreprise est de procéder en étapes : « prêt » (contexte et vision d'ensemble), « feu » (identifier les risques) et « partez » (mise en place de contrôles). La recherche d'Aberdeen montre que les entreprises sont très majoritairement intéressées par la mise en place de contrôles techniques, mais peu sur la préparation du projet (ce qui réduit l'impact et la portée)[80].

Un autre rapport, édité par Ponemon Institute en 2022 met en évidence non plus la fuite de données, mais la survenance d'attaques cyber du fait dont la raison est interne.[81] Les entreprises ayant participé à l'étude ont mené des investigations suite à la survenance d'incident de cybersécurité, permettant d'identifier la cause source : 56% des incidents ont pour source la négligence d'un salarié ou d'un partenaire.



Répartition des sources d'attaques

[79] **COLLINS, Robert. 2021.** Insider Risk Caused By Data Exposure and Leaks Siphons Vast Revenue from Organizations. *BusinessWire*. [En ligne] 07 juillet 2021. [Consulté le 14 avril 2022.] https://www.businesswire.com/news/home/20210707005267/en/Insider-Risk-Caused-By-Data-Exposure-and-Leaks-Siphons-Vast-Revenue-from-Organizations.

[80] **Aberdeen Group. Juin 2021.** *Understanding Your Insider Risk and the Value of Your IP*. Juin 2021.

[81] **Ponemon Institute & Proofpoint. 2022.** *2022 costs of insider threats global report*. 2022.

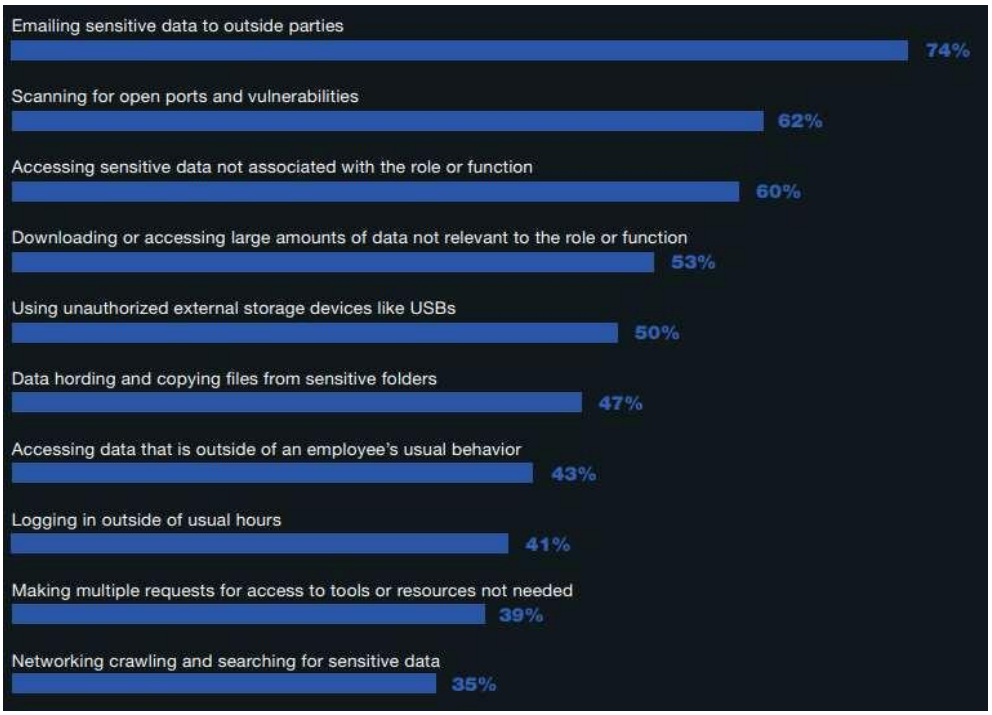
Certains signes ne trompent pas et il est possible de détecter certains signaux afin de savoir si son entreprise est en risque. Les comportements suivants sont souvent en cause lorsqu'il s'agit de menace interne :

- Les salariés ne sont pas suffisamment formés et sensibilisés au niveau de la régulation, des obligations et des bonnes pratiques qui impactent la sécurité de l'entreprise.
- Les salariés ne connaissent pas les modes opératoires qui permettent d'avoir une assurance que le matériel (a fortiori le BYOD) est sécurisé en continu.
- Les salariés envoient des données confidentielles dans des bases de données Cloud non sécurisées et parfois externes à l'entreprise.
- Les salariés ne respectent pas les bonnes pratiques de l'organisation à des fins de simplification de leurs tâches quotidiennes
- La politique de patching / montée de version n'est pas centralisée et pilotée par la DSI, laissant la main aux salariés pour adapter le niveau de sécurité logicielle de leur SI.

b. Les salariés malveillants

Le salarié malveillant peut avoir plusieurs motivations. Il peut avoir pris conscience de la valeur intrinsèque des données de l'entreprise et souhaite en tirer profit en les vendant à la concurrence. Il peut aussi se muer en vengeur, n'ayant pas de visée lucrative mais étant plus attaché par le désir de se faire justice (raisons personnelles ou professionnelles) ou dénoncer certaines pratiques éthiquement contestables ou illicites de l'entreprise.

Le rapport Ponemon permet de lister les principaux canaux de fuite d'information et d'activités frauduleuses réalisées par des salariés malveillants.



Résultat du questionnaire concernant les types d'activités frauduleuses subies par les entreprises participantes

3.2.3.2. Les tiers

Afin d'atteindre certaines cibles, il est plus facile de s'attaquer aux tiers, souvent moins matures et disposant d'accès au réseau de grandes entreprises. Ainsi, les prestataires, qu'il s'agisse de PME, de TPE ou d'entreprises de plus grande dimension, se doivent d'être choisies avec attention afin de ne constituer une menace pour l'entreprise cliente.[82] En effet, l'externalisation de plus en plus importante des services de l'entreprise provoque des interconnexions plus fortes des systèmes d'information entre fournisseurs et clients. La masse de données partagées, parfois sensibles, ne continue d'augmenter et devient difficile à superviser.

Par ailleurs, il est intéressant pour un attaquant de cibler un fournisseur du fait de ses accès aux systèmes d'information de nombreux clients et même d'organismes publics : c'est le principe du « Hack one, breach many ». Nous pouvons citer l'exemple de SolarWinds, dont l'outil Orion, utilisé par 33000 entreprises (dont le gouvernement américain), s'est fait hacker par un APT Russe en vue de déstabiliser tous les clients de l'éditeur. [83]

Pourtant, de nombreuses organisations considèrent l'accès à distance par des tiers comme une menace pour la sécurité, mais pas comme une priorité.

Il est possible de fiabiliser les 6 étapes du cycle de vie du fournisseur[84] :

Cycle de vie des tiers

a. Rechercher et sélectionner (Source & select)
La phase de sélection du prestataire est un procédé très classique et indispensable. Lors de ce processus sont évalués la possibilité de répondre au besoin, la réputation, le coût, le retour sur investissement, l'impact sur la productivité… 51% des entreprises participant à l'étude admettent que le niveau de sécurité et de confidentialité ne fait pas partie des critères de sélection.

En 2020, 31 % des entreprises ont déclaré que le risque cyber lié aux tiers présents sur la chaîne d'approvisionnement ne faisait pas partie de leur analyse des risques. En 2021, ce pourcentage est tombé à 13%.

---

[82] **MEDDAH, Hassan. 2019.** Les sous-traitants, le nouveau maillon faible de la chaîne de la cybersécurité. *L'usine Nouvelle.* [En ligne] 23 janvier 2019. [Consulté le 02 mai 2022.] https://www.usinenouvelle.com/article/les-sous-traitants-le-nouveau-maillon-faible-de-la-chaine-de-la-cybersecurite.N796835.

[83] **S., Elina. 2020.** SolarWinds : tout savoir sur la cyberattaque historique des États-Unis. *Le Big Data.* [En ligne] 22 décembre 2020. [Consulté le 02 mai 2022.] https://www.lebigdata.fr/solarwinds-cyberattaque-historique-usa.

[84] **BlueVoyant. 2021.** *Managing Cyber Risk Across the Extended Vendor Ecosystem*. New York City : BlueVoyant, 2021.

b. Evaluer (Intake and score)

Lorsque le tiers a été sélectionné, il faut bien entendu convenir des détails de la prestation via un contrat comprenant des Service Level Agreement (SLA) et s'accorder sur le niveau de sécurité minimum à respecter. Connaître le niveau de maîtrise de son fournisseur pourrait paraître une évidence, mais 65% des fournisseurs n'ont jamais présenté de certification de sécurité à leur client. Il sera également possible de classifier ces tiers en fonction du risque sécurité qu'ils font peser sur l'entreprise (droits administrateurs ou droits en consultation uniquement).

c. Gestion des identités et des accès (Identity and access management)

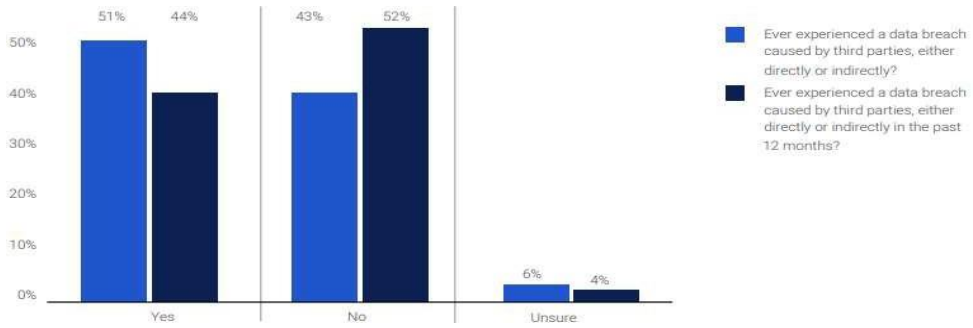
Comme son nom l'indique, il convient après l'analyse de sécurité de fournir des accès au prestataire. Il faut parfois gérer les accès des prestataires différemment de ceux des salariés internes, notamment du fait qu'ils ne font pas partie des systèmes RH, étant souvent le pivot pour le commissionnement et décommissionnement des accès.[85] Par ailleurs, pour des besoins d'agilité, les fournisseurs ont souvent accès au système d'information via des comptes génériques partagés par plusieurs personnes. C'est encore plus risqué pour un infogérant ou un fournisseur de logiciel SAAS maintenant l'infrastructure de son client, et qui a donc accès aux bases de données et aux serveurs de manière non supervisées. Pire, le fournisseur, disposant d'accès administrateurs, peut à son tour ouvrir l'accès du système d'information à ses propres sous-traitants, démultipliant l'impact potentiel.

Il est donc inquiétant de constater que 54 % des entreprises affirment qu'elles ne disposent pas d'un inventaire complet de tous les tiers ayant accès à leur réseau. Pour les salariés comme pour les prestataires, le principe de moindre privilège est fortement recommandé.

d. Sécuriser les connexions (Secure connection)

Il s'agit bien entendu du sujet le plus critique. Pour sécuriser au mieux la connexion des tiers sur le système d'information, les entreprises doivent évaluer le niveau de sécurité des protocoles d'accès et leurs moyens d'identification. Pourtant, 63 % des entreprises déclarent qu'elles n'ont pas de visibilité sur le niveau d'accès et les autorisations des utilisateurs internes et externes : elles ne savent pas identifier exactement qui a accès au réseau et avec quels droits.

La conséquence directe est un risque accru d'attaque et de fuite de données, facilitée par un niveau insuffisant de pilotage et supervision des droits d'accès. 74% des entreprises victime d'une fuite de données causée par un tiers est la conséquence d'un octroi de droits trop étendus.



Fuite de données causées par des tiers disposant d'accès distants

[85] **JONES, Isa. 2022.** 'Hack One, Breach Many' Is Here to Stay: How to Secure Your Third-Party Risks. *Infosecurity*. [En ligne] 26 janvier 2022. [Consulté le 02 mai 2022.] https://www.infosecurity-magazine.com/blogs/how-to-secure-your-thirdparty-risks/.

e. Surveiller et évaluer (Monitor and access)
Lorsque les tiers ont accès au système d'information, il est primordial de mettre en place un processus fiable et permanent de surveillance et d'évaluation de celui-ci.

Bien que conscientes que les tiers ont accès direct à leur données, 59% des entreprises n'utilisent pas d'outils de surveillance et ne contrôlent pas l'activité des tiers. Là encore, les entreprises sont trop peu impliquées dans ce processus et préfèrent se baser sur leur contrat ou sur la réputation du prestataire afin d'avoir une assurance sur le niveau de sécurité.

Plus inquiétant, la part d'entreprise évaluant le niveau de sécurité et de gestion des risques de leurs tiers de manière périodique a baissé entre 2020 (32%) et 2021 (13%). En plus d'une surveillance de l'activité sur le réseau, il est possible d'obtenir de la part des tiers un certain nombre de certifications permettant de démontrer son niveau de maturité (certifications ISO et ISAE).[86]

Reporter et superviser (Report and manage)
Afin de se projeter dans le long terme avec ses tiers, il est important de pouvoir suivre certains indicateurs de performance, surtout lorsque ceux-ci sont impliqués dans des processus métier. Sans reporting, la prise de décision stratégique peut être pénalisée conduisant à des erreurs d'appréciation du risque.

38% des entreprises n'ont aucun moyen de savoir si un incident survient chez leur tiers et 41% n'ont pas de visibilité sur le niveau de résolution d'un incident survenu chez un tiers.

Les « attaques par rebond » sont un moyen efficace d'arriver à ses fins, en s'en prenant à des prestataires plutôt que directement à la cible. Il convient alors de considérer le risque représenté par les tiers comme très élevé et ainsi adapter son mode de gestion des prestations. Les bonnes pratiques sont les suivantes :

- Avoir une vue claire sur toute la chaîne d'approvisionnement et classer les tiers selon leur criticité et leur niveau de maturité.
- Faire l'inventaire des tiers avec qui l'entreprise coopère et des données dont ils ont accès (en lecture ou écriture).
- Mettre en place un organisme de reporting périodique avec des indicateurs clairs et mesurables.
- Suivre l'évolution du risque tout au long de la relation : refuser le risque, réduire le risque, transférer le risque, accepter le risque
- Évaluer le niveau de sécurité des prestataires via l'obtention de certifications

[86] **SecureLink & Ponemon Institute. 2021.** *A crisis in third-party remote access security.* 2021.

3.2.4. Le manque de sensibilisation et de formation

Si les salariés peuvent se sentir non concernés par les enjeux de protection de la donnée et de la cybersécurité, il faut l'avouer, c'est aussi parce que les entreprises jouent le jeu de l'obscurité. En effet, une étude réalisée par HackerOne (entreprise de service de recherche de vulnérabilités) montre que 65% des répondants veulent que leur entreprise paraisse comme infaillible (alors que personne ne l'est) et que 64% font le choix de ne pas communiquer de manière transparente sur leur politique de sécurité avec leurs salariés et leurs partenaires externes. [87]

Être équipé ne signifie pas être protégé, c'est pour cela qu'en plus d'une communication ouverte sur les notions et les besoins de sécurité auprès de tous les salariés, il faut aussi les former.[88] Les mauvaises habitudes ont la vie dure et il est fréquent que les situations suivantes arrivent :

- Partage de mots de passe entre collègues
- Maintien des accès réseau et applicatifs de salariés ayant quitté les effectifs et utilisation de leurs comptes
- Ouverture de liens ou de pièces jointes reçues par email inconnus
- Branchement d'une clé USB trouvée dans la rue sur le poste de travail
- Navigation sur un wifi public sans VPN
- Fournir des données confidentielles à un attaquant réalisant une fraude au fournisseur ou une fraude au président (ingénierie sociale)

Depuis quelques années, la surface d'attaque et de risques n'a cessé d'augmenter, et s'est encore accrue avec la généralisation du télétravail. Là encore, si les salariés considèrent que la sécurité est de la seule responsabilité du service IT, les incidents ne peuvent que survenir. Ainsi les entreprises se doivent-elles de former leurs salariés et leur direction (par ordre de priorité selon la sensibilité de leur fonction occupée).[89] 57% des entreprises rencontrent des difficultés à créer une culture cyber dans son entreprise, y compris au sein de sa propre direction : 28% seulement pensent que leur direction est suffisamment concernée par ce sujet et 10% des membres de direction estiment qu'ils sont suffisamment informés du niveau de sécurité de leur propre organisation)[90].

La formation et la sensibilisation doivent rentrer dans le budget cyber, qui, selon CyberShark représente 6% du budget informatique d'une entreprise, alors qu'il serait conseillé d'y consacrer entre 9% et 14% [91].

---

[87] **HackerOne. 2021.** *The Corporate Security Trap - Shifting security culture from secrecy to transparency*. 2021.

[88] **CPR Asset Management. 2021.** LA CYBERSÉCURITÉ - NOUVEL ENJEU CLÉ POUR LES ENTREPRISES. *CPR Asset Management*. [En ligne] 08 novembre 2021. [Consulté le 27 février 2022.] https://www.cpr-am.fr/Local-content/Actualites-Presse-Recompenses/La-cybersecurite-Nouvel-enjeu-cle-pour-les-entreprises.

[89] **Appitel Beside. 2021.** POURQUOI FORMER VOS SALARIÉS À LA SÉCURITÉ INFORMATIQUE ? *Appitel Beside*. [En ligne] 29 mars 2021. [Consulté le 03 mars 2022.] https://www.appitel.fr/blog/appitel/pourquoi-former-vos-salaries-a-la-securite-informatique/.

[90] **Tanium Inc. and Nasdaq, Inc. 2016.** *THE ACCOUNTABILITY GAP : CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY*. University of London : s.n., 2016.

[91] **CyLumena. 2021.** Four Areas Where You're Spending Too Much and Four Where You're Spending Too Little on Cybersecurity. *CyLumena*. [En ligne] 2021. [Consulté le 04 mars 2022.] https://www.cylumena.com/insights/reallocate-cyber-budget/.

Une fois que vous avez commencé à créer une culture de sensibilisation à la cybersécurité au travail, l'étape suivante consiste à comprendre les rôles spécifiques que chaque individu doit jouer[92] :

Rôles de la direction

- Prioriser les actions à mener en termes de politique de sensibilisation
- Évaluer de manière formelle et périodique des analyses de risques de cybersécurité (techniques et humaines), par des organismes indépendants
- Surveiller les résultats et suivre les indicateurs de performance à travers le temps pour établir une tendance (amélioration ou régression)

Rôles des cadres

- Organiser la coordination des efforts de cybersécurité et intégrer la sécurité dans les processus quotidiens des équipes
- Communiquer sur les bonnes pratiques et montrer l'exemple
- Participer aux tests et exercices de sécurité de manière périodique

Rôles du personnel

- Assister à tous les événements de formation du personnel
- Rester attentif et à jour en consultant l'actualité des modes opératoires des attaquants.
- Appliquer ce qui a été appris en formation pour toutes les activités quotidiennes

Un manque de transparence, de sensibilisation et de formation a des conséquences dommageables certaines pour la pérennité et la performance des entreprises. Pourtant, quelques pistes peuvent être envisagées :

- Construire une culture de l'ouverture et éviter de chercher un coupable lorsqu'un incident se déclare
- Considérer la sécurité et sa diffusion non plus comme un centre de coûts mais comme un investissement stratégique
- Donner accès à tous les salariés le processus clair de remontée de vulnérabilités
- Mettre en place un « trust center » synthétisant toutes les informations sur l'approche de la sécurité, la confidentialité et la conformité, ou plus simplement distribuer des « trusts reports » périodiques décrivant les mesures qui sont mises en place en termes de sécurité et présentant les vulnérabilités qui ont été résolues
- Former ses salariés via des MOOCs et réaliser des tests de phishing

[92] **OLSON, Jason. 2022.** Why Cybersecurity Awareness in the Workplace is Everyone's Business. *EideBailly*. [En ligne] 2022. [Consulté le 04 mars 2022.] https://www.eidebailly.com/insights/articles/legacy/cyber-from-the-break-room-to-the-board-room.

3.2.5. Gestion de son image et de sa réputation

3.2.5.1. La e-réputation

Dans le contexte de guerre informationnelle que se livrent les entreprises, il est important de tout faire afin de maîtriser au mieux son image. Dans un monde connecté par les technologies actuelles, la réputation se joue sur le terrain numérique, on parle alors d'e-réputation.

L'e-réputation représente l'image qu'une personne physique ou morale a su générer sur Internet, du prisme des internautes.[93] Il est donc évident qu'une entreprise doit être consciente que ces actions, ses choix, sa politique vont orienter favorablement ou défavorablement l'opinion du public. D'ailleurs, cette opinion peut s'enflammer et échapper à tout contrôle de l'entreprise. En tant que potentiel client ou partenaire, il est tout naturel de s'enquérir de la réputation d'une entreprise en se connectant à internet et en réalisant les recherches idoines.

L'e-réputation a donc un impact très important : tant que les prospects n'auront pas expérimenté le service / produit proposé, ils se seront d'abord basés sur leur perception de la marque.[94] C'est l'image de marque que l'entreprise doit cultiver. Si cette image de marque répond aux attentes du client, celui-ci en deviendra lui-même un vecteur, renforçant positivement la réputation de l'entreprise (73% des Français ont déjà laissé un avis client sur un site Internet)[95]. Or, les internautes ont tendance à spontanément faire confiance aux retours utilisateurs qu'ils rencontrent en naviguant sur internet. Une mauvaise image de marque aura des impacts indirects sur le chiffre d'affaires (perte de part de marché). 96% des consommateurs connectés sont influencés par un avis négatif sur un produit. Sur ces 96%, 30% renoncent à l'achat ou choisissent le produit d'un concurrent alors que 66% reportent leur achat. [96]

Plus globalement, une réputation négative peut être tout à fait légitime, du fait de services / produits de mauvaise qualité ou d'un environnement de travail délétère par exemple. Au contraire, la dégradation de l'image de marque peut tout à fait être injuste et découler d'actions de dénigrement et de déstabilisation de la part de concurrents ou tierce partie (se référer à la partie Infox et déstabilisation).

« En politique, ce qui est cru devient plus important que ce qui est vrai. » - Charles-Maurice de Talleyrand-Périgord.

La formule bien connue de Talleyrand est valable pour le domaine économique et réputationnel.

---

93 **Journal Du Net. 2019.** E-réputation : définition, synonyme et traduction. *Journal Du Net.* [En ligne] 13 mars 2019. [Consulté le 15 mars 2022.] https://www.journaldunet.fr/business/dictionnaire-du-marketing/1207880-e-reputation-definition-et-traduction/#:~:text=D%C3%A9finition%20du%20mot%20e%2Dreputation,r%C3%A9seaux%20sociaux%2C%20blogs%20ou%20forums..

94 **Qualtrics. 2022.** Brand perception: Everything you need to know. *Qualtrics XM.* [En ligne] 2022. [Consulté le 15 mars 2022.] https://www.qualtrics.com/uk/experience-management/brand/brand-perception/?rid=ip&prevsite=fr&newsite=uk&geo=FR&geomatch=uk.

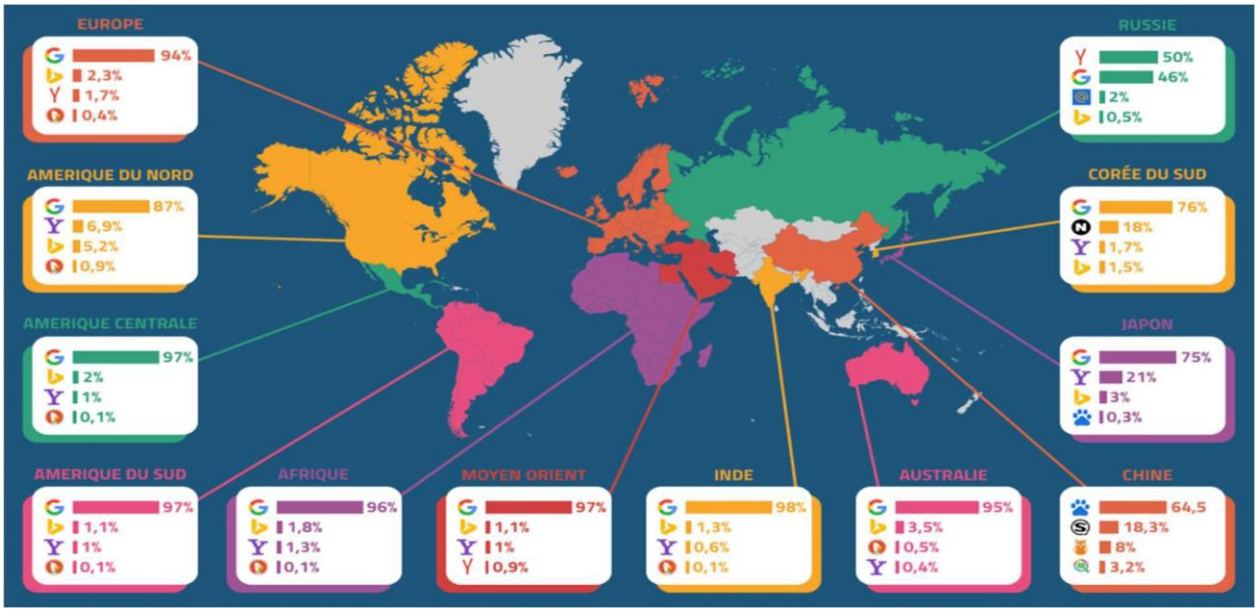
95 **COHEN, Eloïse. 2020.** Infographie Que pensent les Français des avis clients? *eMarketing.* [En ligne] 03 janvier 2020. [Consulté le 12 mars 2022.] https://www.e-marketing.fr/Thematique/retail-1095/Infographies/Que-pensent-Fran-ais-avis-clients-345324.htm

96 **Digimind. 2022.** L'impact déterminant de la réputation en phase d'achat : l'histoire du VTT d'Arthur. *Digimind.* [En ligne] 18 février 2022. [Consulté le 12 mars 2022.] https://blog.digimind.com/fr/insight-driven-marketing/impact-determinant-de-reputation-en-phase-dachat.

Ainsi les entreprises doivent-elle redoubler de vigilance et gérer leur image via les canaux suivants[97] :

Les moteurs de recherche

Nous pouvons citer Google, Bing, Baidu, Yahoo, Yandex, DuckDuckGo, Qwant et bien d'autres. Il faudra consulter les moteurs de recherche les plus utilisés selon le positionnement géographique de l'entreprise : Google est le principal moteur de recherche, mais Yandex est prisé par les zones russophones et Baidu par la Chine (où Google est interdit).



Part de marché des moteurs de recherche dans le monde (source StatCounter)[98]

A savoir : le positionnement du site internet et de l'information relative à l'entreprise doit se trouver dans les premières pages des résultats, appelées « page de notoriété ». Au-delà, l'information à tendance à se perdre car les internautes ne se donnent pas la peine de pousser leur investigation (67% des clics sont faits sur les cinq premiers résultats). En effet, les algorithmes des moteurs de recherche sont conçus pour valoriser et mettre en avant les contenus plébiscités par les internautes[99]

Afin d'optimiser la captation d'information réalisée sur les moteurs de recherche (via différentes techniques), se référer au chapitre sur l'aspect offensif de la guerre de l'information.

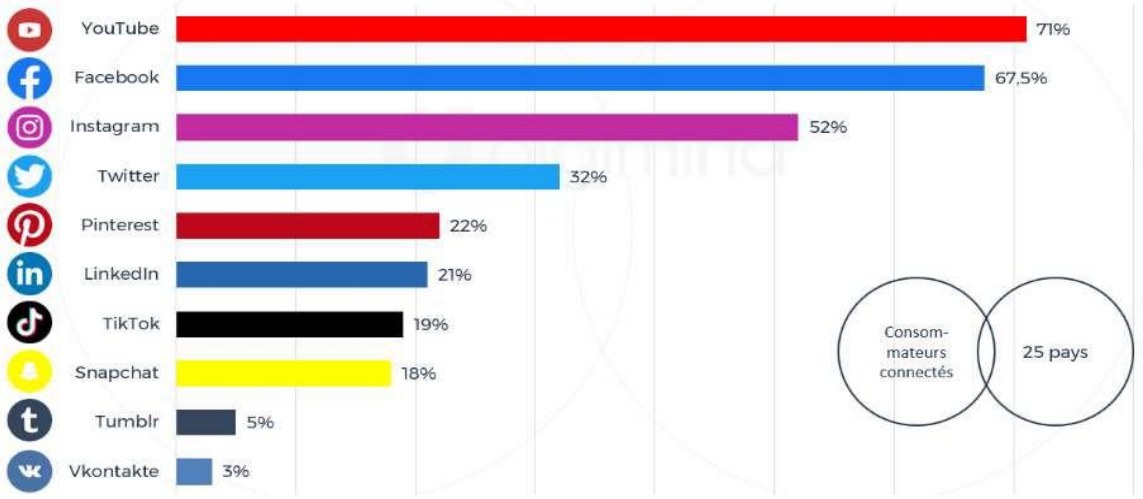
Les réseaux sociaux

[97] **Semji. 2022.** Comment maîtriser son e-réputation ? *Semji*. [En ligne] 2022. [Consulté le 12 mars 2022.] https://semji.com/fr/guide/e-reputation/.

[98] **Opinion Act. 2019.** Parts de marché des moteurs de recherche dans le monde. *Opinion Act*. [En ligne] 2019. [Consulté le 12 mars 2022.] https://www.opinionact.com/ressources/seo-content-marketing/parts-de-marche-des-moteurs-de-recherche-dans-le-monde.

[99] **Les Echos Entrepreneurs. 2014 .** Zones de description et notoriété des pages. *Les Echos*. [En ligne] 14 mai 2014 . [Consulté le 12 mars 2022.] https://business.lesechos.fr/entrepreneurs/web/dossiers/4174762/tpepme-0004174762-2-zones-de-description-et-notoriete-des-pages-63781.php.

Les consommateurs aussi bien que les entreprises prennent leurs décisions en consultant les tendances qui se dégagent sur les réseaux sociaux : une étude menée sur 67000 utilisateurs dans 25 pays montre que 72% des consommateurs connectés utilisent les réseaux sociaux au moins une fois par jour. Ce vecteur de communication peut permettre de donner son avis mais aussi de rayonner via l'organisation d'évènements et de campagnes marketing. Les entreprises vont alors investir dans la mise en place d'un service de Community Management, qui interagira directement avec la clientèle et les partenaires. Certains réseaux ont une visée plus professionnelle (ex : LinkedIn) et d'autres seront plus grand public (ex : Facebook).



Top 10 des réseaux sociaux dans le monde – Source : Kantar TGI Global Quick View Report 2020 [100]

Les blogs et forums

Dans l'antiquité, les forums représentaient une place ouverte, un espace d'échanges et de partage entre citoyens. Aujourd'hui, le forum sur internet a conservé sa nature initiale et constitue toujours un véritable lieu de discussions libres sur un sujet, une marque ou une expérience vécue. Un chef d'entreprise se devra d'être présent sur les blogs et forums afin de connaître les idées, les perceptions et les désidératas des consommateurs afin d'identifier si des rumeurs sont créées ou s'il faut adapter sa stratégie de communication en vue de renforcer l'adhésion des clients.

Les influenceurs

Ce qui semblait être un épiphénomène il y a 15 ans, l'impact des influenceurs sur les modes de consommation n'est plus à prouver. On trouve aujourd'hui des profils variés comme des célébrités, des experts / leaders d'opinion/ journalistes, des blogueurs et des micro-influenceurs. L'utilisation d'un service d'influenceur se révèle payant puisque travailler avec un influenceur peut créer peut générer un retour sur investissement 11 fois supérieur à celui du marketing digital traditionnel.[101] En effet, 75 % des consommateurs connectés ont déjà acheté un produit après avoir écouté les conseils / avis d'un

[100] **ASSELIN, Christophe. 2021.** Les réseaux sociaux en France et dans le monde : les chiffres d'utilisation en 2021. *Digimind*. [En ligne] 21 avril 2021. [Consulté le 12 mars 2022.] https://blog.digimind.com/fr/tendances/r%C3%A9seaux-sociaux-france-monde-chiffres-utilisation-2021.

[101] **Net Offensive. 2018.** Influenceurs et e-réputation de l'entreprise et marque en ligne. *Net Offensive*. [En ligne] 2018. [Consulté le 12 mars 2022.] https://www.netoffensive.blog/e-reputation/ameliorer/influenceurs/.

influenceur. A contrario, un influenceur dénigrant l'image d'une marque peut constituer un véritable risque et des pertes de part de marché.[102]

Les portails d'évaluation

Les internautes peuvent aussi faire part de leur avis et de leurs commentaires sur des plateformes d'évaluation comme Google My Business, Tripadvisor, Yelp, Trustpilot… Attention toutefois, car la Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes estime que le processus de faux avis est devenu légion polluant à hauteur de 20% les avis en encensant une entreprise ou au contraire en la discréditant.[103]

3.2.5.2. La défense contre l'infox et les tentatives de déstabilisation

En cas d'impair, il se peut qu'une entreprise ne soit confrontée à un bad buzz, engendrant une crise communicationnelle (due à une maladresse ou un malentendu), une crise structurelle (discrédit d'un produit ou d'un service) ou une crise émotionnelle (morale ou éthique). [104] Face à cette situation, l'entreprise, accompagnée d'un service de communication de crise ou non, pourra ne pas réagir (amplifiant certainement l'effet négatif), supprimer le contenu (très mal vu car interprété comme un aveu) ou en répondant de manière ouverte (en réfutant un argument ou en faisant amende honorable). La réaction doit se faire de manière très réfléchie car tout nouvel impair lié à cette communication ne pourrait qu'alimenter sa propre paralysie[105].

D'après Christian Harbulot, « Internet se révèle être l'instrument idéal pour véhiculer une rumeur, diffusée en temps réel, à l'échelle de la planète. Le management de crise ne suffit plus pour enrayer une tentative de déstabilisation »[106]. Ainsi, lorsque le bad buzz est le fruit d'un comportement malveillant, on peut en déduire qu'une tentative de déstabilisation est en cours.

Les attaquants ont recours aux infox (fake news en anglais). La Commission d'enrichissement de la langue française a défini l'infox comme une information mensongère ou délibérément biaisée servant à défavoriser un parti politique, à entacher la réputation d'une personnalité ou d'une entreprise, ou à contrer une vérité scientifique établie.[107] Les dégâts sociaux que peuvent provoquer les infox peuvent provoquer des impacts dans le monde physique (manifestations, conflits ou intention de vote) et économique.[108] Les entreprises vont donc pouvoir utiliser l'arme de la désinformation comme avantage concurrentiel pour discréditer les entreprises. La régulation des infox est bel et bien reconnue comme un

[102] **SALGUES, Floriane. 2017.** Quel est l'impact des influenceurs sur les consommateurs ? *eMarketing*. [En ligne] 18 octobre 2017. [Consulté le 12 mars 2022.] https://www.e-marketing.fr/Thematique/social-media-1096/Infographies/Quel-est-impact-influenceurs-consommateurs-322071.htm#.

[103] **SIX, Nicolas. 2022.** Cinq étoiles et 10/10 : pourquoi il ne faut pas faire confiance aux notes des internautes. *Le Monde*. [En ligne] 19 janvier 2022. [Consulté le 12 mars 2022.] https://www.lemonde.fr/pixels/article/2022/01/19/cinq-etoiles-et-10-10-pourquoi-il-ne-faut-pas-faire-confiance-aux-notes-des-internautes_6110162_4408996.html.

[104] **Semji. 2014.** Bad buzz intentionnel : quand les marques surfent sur le buzz négatif. [En ligne] 2014. [Consulté le 12 mars 2022.] https://semji.com/fr/blog/bad-buzz-intentionnel-quand-les-marques-surfent-sur-le-buzz-negatif.

[105] **MOINET, Nicolas. 2020.** Les sentiers de la Guerre Economique 2 «Soft Powers». Versailles : VA Editions Collection «Indiscipliné», 2020. p. 100. ISBN 978-2-36093-117-0.

[106] **La Tribune. 2001.** *Un seul homme peut déstabiliser une multinationale*. 11 avril 2001. Propos de Christian Harbulot recueillis par Sandrine L'Herminier.

[107] **Ministère de la Culture. 2018.** FAKE NEWS. *Ministère de la Culture*. [En ligne] 4 octobre 2018. [Consulté le 12 mars 2022.] http://www.culture.fr/Ressources/FranceTerme/Recommandations-d-usage/FAKE-NEWS.

[108] **CHAIEHLOUDJ, Walid. 2018.** Fake news et droit de la concurrence : réflexions au prisme des cas Facebook et Google. *Cairn.info*. [En ligne] Revue internationale de droit économique , 09 juillet 2018. [Consulté le 12 mars 2022.] https://www.cairn.info/revue-internationale-de-droit-economique-2018-1-page-17.htm?contenu=auteurs.

sujet majeur à l'ère du numérique puisque même des algorithmes gérés par l'intelligence artificielle peuvent aggraver leur propagation. Il peut se présenter sous la forme d'un contenu trompeur, manipulé, fabriqué ou sorti de son contexte.

Idem pour la malinformation qui consiste en la diffusion d'informations vérifiées et véridiques dans l'intention de nuire.[109] C'est typiquement ce qui est en jeu dans le cadre du dénigrement commercial[110] (se référer au chapitre sur le cadre légal pour plus de détails). Pour ce faire, le dénigreur va répandre des informations malveillantes (infox ou malinformation) sur les produits et / ou les services de l'entité visée.

A la marge, il faut aussi considérer la mésinformation, qui est une mauvaise information, qualitativement imparfaite en raison d'erreurs de différentes natures (précipitation et absence de vérification, superficialité de traitement et incomplétude, non-actualisation de contenus et obsolescence, faux pour faire rire), qui, bien que n'ayant aucun but malveillant, peut tout de même être dommageable si les internautes ne réalisent pas de fact-cheking.[111]

Une politique de déstabilisation de la part d'un concurrent pourra même être suivie par des actions de parasitisme (se référer au chapitre sur le cadre légal pour plus de détails). En utilisant la notoriété d'une entreprise (ou justement sa perte de notoriété), un concurrent déloyal pourra en tirer un profit du fait de la récupération des parts de marché perdues via la campagne de désinformation / malinformation.

Les opérations de déstabilisation et d'influence ne s'arrêtent pas à répandre des rumeurs ou des informations, mais peuvent aussi être la caisse de résonance de véritables attaques informatiques .

Affaiblie par un rançongiciel, la crédibilité d'une entreprise peut encore être plus écornée par un concurrent qui communiquerait sur cette situation, étant peut-être lui-même l'instigateur de l'attaque. Comme le souligne Stéphane Nappo (RSSI du groupe SEB) : « il faut 20 ans pour construire une réputation et un cyber-incident de quelques minutes pour la ruiner ».

En définitive, le sujet de l'image d'une entreprise est un sujet pointu et très sérieux. A moins d'être un expert dans ce domaine, les entreprises auront intérêt à se rapprocher de l'Autorité de la concurrence, d'avocats spécialisés dans le droit de la concurrence, d'un cabinet de gestion de l'image / e-réputation et dans un cabinet de communication de crise (pour se préparer en amont, comme n'importe quel plan de continuité d'activité).

Le rapport de la commission dirigé et publié par Gérald Bronner en 2022 sur les désordres informationnels sur les réseaux sociaux titré « Les lumières à l'ère numérique » permet aussi d'avoir de nombreuses pistes de réflexion. [112]

[109] **SILINI, Alberto. 2019.** Cinquante nuances de désinformation. *EJO*. [En ligne] 28 novembre 2019. [Consulté le 14 mars 2022.] https://fr.ejo.ch/deontologie-qualite/cinquante-nuances-desinformation-fakenews-trouble-information-claire-wardle-manipulation.

[110] **GHERARDI, Alexandra. 2014.** Le dénigrement commercial et la diffamation, une subtile différence. *avocats-picovschi*. [En ligne] 20 octobre 2014. [Consulté le 12 mars 2022.] https://www.avocats-picovschi.com/le-denigrement-commercial-et-la-diffamation-une-subtile-difference_article_948.html.

[111] **MARTIN, Isabelle. 2021.** FAKE NEWS, INFOX, DE QUOI PARLE-T-ON ? *Clemi*. [En ligne] 2021. [Consulté le 12 mars 2022.] https://www.clemi.fr/fr/evenements/operations-speciales/exposition-fake-news-art-fiction-mensonge/la-fabrication-des-fake-news/fake-news-infox-de-quoi-parle-t-on.html.

[112] **BRONNER, Gérald. Janvier 2022.** *Les Lumières à l'ère numérique*. Paris : Rapport de la Commission, Janvier 2022.

3.2.5.3. L'importance de la prise de conscience de l'encerclement cognitif

La guerre de l'information que se livrent les États et les entreprises se jouent de manière micro et macro-économique[113]. En effet, on parle d'encerclement cognitif pour une démarche, non visible, de ou des attaquants visant leur cible, sans que celle-ci ne puisse savoir d'où l'attaque provient directement. Il a pour but de détruire la légitimité, la crédibilité, et l'image de sa cible. Certains pays comme les États-Unis, l'Allemagne ou la Chine l'utilisent volontiers afin d'assurer leur suprématie dans le domaine économique.

La France, elle, se limite dramatiquement aux actions défensives en ce qui concerne la protection de ses intérêts économiques et stratégiques. Là où d'autres pays vont miser sur l'agressivité et la déstabilisation, la France (acteurs publics et privés) vont adopter une posture plus passive, retranchée derrière un idéal d'éthique, en pensant que « les bons comptes font les bons amis ». Or, la déstabilisation peut provenir de pays amis et de partenaires de toujours : les outils purement défensifs et la veille ne peuvent alors pas suffire.

La notion d'encerclement cognitif est essentielle car elle peut aider à identifier la source des tentatives de déstabilisation. Semblant trop lointains pour influencer, les risques liés à cet encerclement cognitif doit être pris au sérieux par la classe politique autant que par les chefs d'entreprises : les think tanks, les lobbys et les ONG sont des outils très efficaces permettant d'influer sur les tendances économiques d'un marché globalisé ou local.

D'ailleurs, les ONG sont étroitement surveillées par la Direction du Renseignement et de la Sécurité de la Défense (DRSD), car leur popularité favorable auprès du grand public occulte facilement l'instrumentalisation dont ces organisations sont victimes (ou complices) dans le cadre de la déstabilisation d'acteurs économiques.

- Rafale : Des ONG, dont la Fédération internationale pour les droits humains (FIDH), L'Observatoire des Armements (OBSARM) ou la Cairo Institute for Human Rights Studies (CIHRS) sont insurgés contre la vente d'un total de 54 Rafales. Cependant, aucun article ne dénonce l'achat de 20 Soukhoï SU-35 par l'Egypte à la Russie. Ainsi cette déstabilisation venue de l'étranger vient faire vaciller les opportunités d'investissement des banques qui ne souhaitent pas subir l'ire des ONG[114].

- Secteur agro-alimentaire – l'exemple du lait et de la viande : Là encore, des ONG comme L214 peuvent agir pour saper la réputation d'une filière toute entière. Seulement, il convient de se demander à qui profite la situation. Les potentiels commanditaires sont les agents économiques souhaitant maintenir les prix du lait au plus bas (les transformateurs et les distributeurs) et les concurrents comme les céréaliers ou les entreprises d'innovation / laboratoires produisant de la viande de synthèse.

Enfin, les Think Tanks jouent un rôle important[115]. Les Think Tanks, considérés comme neutres aux yeux du grand public, sont des instituts de recherche qui peuvent avoir des airs de lobbies intellectualisés[116]. Les études réalisées par ces groupes vont influencer un environnement donné aussi bien qu'un pouvoir

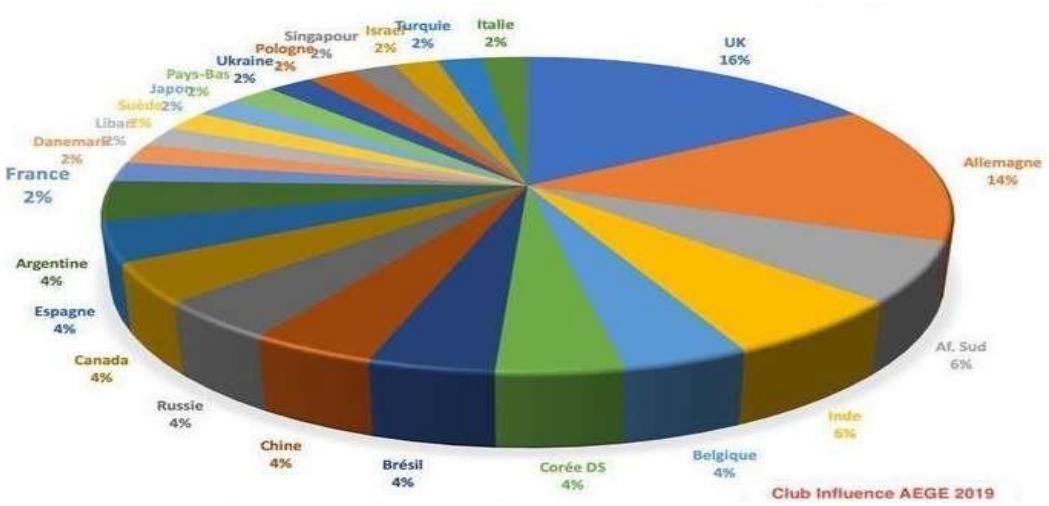
[113] **CATHARING. 2020.** L'encerclement cognitif, mode d'emploi. *Olduvaï.* [En ligne] 10 février 2020. [Consulté le 02 mai 2022.] https://www.le-projet-olduvai.com/t11696-l-encerclement-cognitifmode-d-emploi.

[114] **FÉDÉRATION INTERNATIONALE POUR LES DROITS HUMAINS. 2018.** Egypte : une répression made in France. *FIDH*. [En ligne] 02 juillet 2018. [Citation : 26 avril 2022.] https://www.fidh.org/fr/regions/maghreb-moyen-orient/egypte/egypte-une-repression-made-in-france.

[115] **Ecole de Guerre Economique (MSIE36). 2021.** Comment les États-Unis contribuent-ils à affaiblir l'économie française ? *EGE.* [En ligne] v12.1, Octobre 2021. [Consulté le 02 mai 2022.] MSIE36 sous la direction de Christian HARBULOT. https://www.ege.fr/sites/ege.fr/files/media_files/rapport_alerte_usa_2021.pdf.

[116] **FERRIA, Haroun et VACHEL, Julien. 2019.** Les think tanks français : des lobbies intellectualisés ? *portail-ie*. [En ligne] 11 février 2019. [Consulté le 02 mai 2022.] https://portail-ie.fr/analysis/2061/les-think-tanks-francais-des-lobbies-intellectualises.

exécutif ou l'opinion publique. Rien d'étonnant que ces regroupements d'experts ne soient utilisés comme des armes d'influence par les États-Unis, qui représentent 1/3 des Think Tanks au niveau mondial.



Répartition géographique des Think Tanks non-US en 2017

Chercher à qui profite le crime, telle doit être la question que se pose celui ou celle qui veut connaître la source d'une opération de déstabilisation ou d'influence[117]. L'instigateur d'une attaque informatique et / ou informationnelle, fragilisant la réputation et l'environnement économique ou informatique peut, bien entendu, être le concurrent, mais la source peut aussi être bien plus indirecte.

3.2.6. Protection de ses noms de domaine

Succinctement, il est possible de décrire les DNS comme des composants utilisés pour associer les services basés sur internet (site web, hébergement, emails) à un nom de domaine.[118] Plusieurs étapes se doivent d'être suivies pour avoir son nom de domaine :

- Enregistrer le domaine auprès d'un bureau d'enregistrement de domaine (ou registraire de domaine).
- Le bureau d'enregistrement de domaine spécifie le nom de domaine et les ajoute aux des serveurs de noms (qui stockent les enregistrements DNS).
- Les enregistrements DNS sont propagés pour associer le domaine à chaque service web.

Ainsi, le nom de domaine est l'adresse du site internet d'une entreprise, c'est grâce à lui que les internautes peuvent y accéder. En cas de plusieurs sites internet, il conviendra d'avoir plusieurs noms de domaines.

Or, avoir réservé un nom de domaine ne signifie pas qu'il soit sécurisé. En effet, plusieurs risques et dérives liés au nom de domaine existent.

[117] **ASTIER, Stéphane et POUJOL, Axelle . 2019.** Cybersécurité : comment lutter contre les opérations de déstabilisation et d'influence ? *info.haas-avocats*. [En ligne] 2019. [Consulté le 03 mai 2022.] https://info.haas-avocats.com/droit-digital/cybersecurite-comment-lutter-contre-les-operations-de-destabilisation-et-d-influence.

[118] **KINSTA. 2020.** Que sont les DNS ? Explication du système de noms de domaine. *KINSTA*. [En ligne] 6 janvier 2020. [Consulté le 20 mars 2022.] https://kinsta.com/fr/base-de-connaissances/que-sont-les-dns/.

3.2.6.1. Perte de son nom de domaine [119]

Tout titulaire d'un nom de domaine est périodiquement confronté à l'obligation de le renouveler au risque de le perdre. Même Google a vu son nom de domaine Google.com racheté pour la somme de 12$ par un internaute après avoir oublié de le renouveler.[120] Pourtant, après la date d'expiration s'ouvre la « Renewal Grace Period », qui varie de 0 à 45 jours selon l'extension du domaine (28 jours pour le .fr), lors de laquelle les entreprises peuvent renouveler le nom de domaine sans risque de le perdre (bien que le site ne soit plus accessible).

Ainsi les entreprises doivent-elles surveiller de près la date de renouvellement, au risque qu'un concurrent achète sciemment le nom domaine d'une entreprise dans le but de détourner la clientèle. Ce mode opératoire est bien entendu frauduleux et condamnable en tant que concurrence déloyale, obligeant la partie accusée de verser des dommages et intérêts. Néanmoins, le transfert du nom de domaine pouvant être long, le préjudice subi par une perte momentanée de son nom de domaine peut durablement impacter les finances de l'entreprise.

Par ailleurs, le rachat de noms de domaines expirés est un véritable marché. En effet, il est possible de consulter le WhoIs du nom de domaine et de les racheter afin de bénéficier de tous l'historique lié au site et des informations internes potentiellement confidentielles.

```
domain:      ege.fr
status:      ACTIVE
hold:        NO
holder-c:    ADLE547-FRNIC
admin-c:     ANO00-FRNIC
tech-c:      OVH5-FRNIC
zone-c:      NFC1-FRNIC
nsl-id:      NSL93567-FRNIC
registrar:   OVH
Expiry Date: 2024-11-28T14:32:27Z
created:     2006-02-10T12:50:30Z
last-update: 2021-11-01T16:28:25Z
source:      FRNIC
```

Exemple de recherche sur le site who.is à propos du nom de domaine « ege.fr »

[119] **Avocats Picovschi . 2016.** Mon concurrent a réservé mon nom de domaine : quels sont mes recours ? *Avocats-Picovschi* . [En ligne] 23 mars 2016. [Consulté le 20 mars 2022.] https://www.avocats-picovschi.com/mon-concurrent-a-reserve-mon-nom-de-domaine-quels-sont-mes-recours_article_1159.html.

[120] **INLEX IP EXPERTISE. 2015.** Quand Google perd son nom de domaine « google.com. *INLEX IP EXPERTISE*. [En ligne] 19 octobre 2015. [Consulté le 20 mars 2022.] https://ip-talk.com/2015/10/19/quand-google-perd-son-nom-de-domaine-google-com/.

3.2.6.2. Cybersquatting

Le cybersquatting consiste en l'achat d'un nom de domaine proche de celui détenu par une entreprise afin de tromper la clientèle (récupération ou arnaque) ou faire du chantage.

Premier cas, un individu ciblant une entreprise ABC, qui dispose du nom de domaine ABC.com va acheter le nom de domaine ABC.fr. Ainsi, l'achat des autres extensions .fr, .eu, .org par un concurrent peut s'avérer pénalisant. Bien qu'acheter toutes les extensions de nom de domaine ne soit pas réalisable dû au très grand nombre d'extension, il sera conseillé, lors de l'ouverture d'un site internet, d'acquérir les principales extensions selon la zone géographique[121].

Deuxième cas, le typosquatting, qui consiste à acheter un nom de domaine très proche de celui d'un site tout à fait légitime, dans le but de tromper[122]. Cela peut se matérialiser par :

- L'ajout de lettres ou de fautes : Gooogle.com avec 3 « o » au lieu de 2.
- L'utilisation du point suscrit (Ḟ pour Ferrari), du point souscrit (ị pour uṇiversal.com) ou de la cédille (Ç pour Çola-Cola)
- Une modification contextuelle de l'URL afin de tromper : Google-recherche.fr

Il s'agit d'une technique très efficace car une étude de Menlo Security estime que 19% des typosquatters ont réussi à faire classer leur site dans la liste des sites de confiance[123]. Cette technique induit les risques d'infox, d'installation de Malware, et de Phishing.

3.2.6.3. Infox

Les infox, comme les autres types de duperies, se propagent notamment car les internautes n'ont pas le réflexe de vérifier les noms de domaines. L'impact sur l'image peut être important.

Nous pouvons citer 2 exemples :

- Vinci a vu en 2016 le cours de son action chuter de 18% car des communiqués envoyés à des médias, venant des adresses « vinci-group» et « vinci.group », affirmaient que des malversations à hauteur de 3,5 milliards d'euros avaient eu lieu en 2015. Les attaquants avaient copié les sites du groupe, permettant de rendre crédible leur mensonge vis-à-vis des journalistes tentant de confirmer cette version[124].

- En 2016, un article prétendument écrit par Associated Press (apnews.com) est apparu sur un site diffusant des fakes news (abcnews.com.co). Le typosquatting a permis de mettre en place un nom de domaine à cheval entre Associated Press et ABC News, autre média américain (abcnews.go) afin de répandre la rumeur selon laquelle quelqu'un avait dû payer 3500$ pour protester contre les rassemblements pro Trump[125].

---

[121] **Journal Du Net. 2021.** Cybersquatting : définition, exemples et textes de loi. *Journal Du Net*. [En ligne] 21 décembre 2021. [Consulté le 20 mars 2022.] https://www.journaldunet.fr/business/dictionnaire-du-droit-des-affaires/1507643-cybersquatting-definition-exemples-et-textes-de-loi/.

[122] **AUTISSIER, Charlotte. 2021.** Nom de domaine : pourquoi et comment l'enregistrer ? Legalstart. [En ligne] 26 mai 2021. [Consulté le 20 mars 2022.] https://www.legalstart.fr/fiches-pratiques/astuces-entrepreneurs/nom-de-domaine/#:~:text=La%20d%C3%A9finition%20d'un%20nom,acc%C3%A9der%20%C3%A0%20un%20site%20internet.

[123] **Menlo Security. 2018.** HOW CYBERCRIMINALS ARE EXPLOITING TRADITIONAL MEASURES OF TRUST. [En ligne] 5 février 2018. [Consulté le 20 mars 2022.] https://info.menlosecurity.com/rs/281-OWV-899/images/Menlo_TrustHacking_Infographic_Final.pdf.

[124] **RIEß-MARCHIVE, Valéry. 2016.** Vinci victime d'une arnaque bien organisée. *Le Mag IT*. [En ligne] 23 novembre 2016. [Consulté le 21 mars 2022.] https://www.lemagit.fr/actualites/450403436/Vinci-victime-dune-arnaque-bien-organisee.

[125] **WEISE, Elizabeth. 2016.** Hackers use typosquatting to dupe the unwary with fake news, sites. *USA Today Tech*. [En ligne] 01 décembre 2016. [Consulté le 20 mars 2022.] https://eu.usatoday.com/story/tech/news/2016/12/01/hackers-use-typo-squatting-lure-unwary-url-hijacking/94683460/.

3.3.6.4. Phishing

Bien qu'il existe des techniques complexes de phishing, que même un internaute attentif n'arrive pas à identifier (ex : détournement de trafic IP via protocole de routage BGP), les attaquant vont avoir tendance à utiliser des techniques simples[126].

En effet, en se faisant passer pour un site de confiance, l'attaquant va compter sur la négligence de la victime pour obtenir un grand nombre d'informations personnelles, commerciales ou sur une organisation. Presque toujours, les internautes sont dupés par une demande de confirmation d'IBAN par ce qu'ils pensent être le service paie, une notification importante du service des impôts ou le gain d'un voyage.

En 2018, le site « airfrance.com » proposait de gagner un billet d'avion d'une valeur de 500€. Cette supercherie permettait aux malfaiteurs d'obtenir les informations personnelles des personnes participant au soi-disant concours[127].

Cette technique fait directement écho au chapitre relatif à la menace interne représentée par les salariés négligents. 32% des violations de données utilisent le phishing. Les salariés vont parfois donner sciemment leur identifiant / mot de passe d'entreprise, que l'attaquant utilisera pour une infiltration sur le réseau, en utilisant ce compte légitime. Le phishing peut alors dégénérer en phishing latéral, l'attaquant utilisant le compte légitime piraté de prime abord pour communiquer et duper des collègues ou des partenaires externes (la fraude au fournisseur ou au président devient alors très probable)[128].

Enfin, les attaquants peuvent se faire passer pour des registraires de domaines vous demandant de vous connecter à votre compte afin de renouveler le nom de domaine. Cela permettrait à l'attaquant, grâce au phishing, de récupérer les moyens de connexion au compte lié au nom de domaine. Ainsi, il faut être vigilant en se connectant toujours directement sur un site en passant par un navigateur plutôt que de suivre un lien dans un mail.

3.2.6.5. Malware

Le cybersquatting peut aussi être utilisé afin de propager des malwares[129]. En effet, les internautes peuvent se faire duper par l'apparence d'un site frauduleux et télécharger volontairement un logiciel malveillant, qui pourra donner accès à des données personnelles et interne à une entreprise (logiciel espion), créer une porte dérobée (Trojan) ou chiffrer les données (rançongiciel). Cela est particulièrement probable si les utilisateurs sont administrateurs de leur poste. Sans administrateur central, les utilisateurs peuvent installer des logiciels non sécurisés. Sans ces accès administrateurs, seuls les logiciels approuvés et disponibles via un catalogue d'application pourront être installés sans l'autorisation d'un administrateur.

---

[126] **AFNIC. 2018.** Cybersquatting, Spam, Phishing… les différents types d'abus sur noms de domaine. [En ligne] 06 septembre 2018. [Consulté le 20 mars 2022.] https://www.afnic.fr/observatoire-ressources/papier-expert/cybersquatting-spam-phishing-les-differents-types-dabus-sur-noms-de-domaine/.

[127] **BANCAL, Damien. 2018.** Fraude aux couleurs d'Air France. *Zataz*. [En ligne] 13 février 2018. [Consulté le 21 mars 2022.] https://www.zataz.com/fraude-aux-couleurs-dair-france/.

[128] **Barracuda. 2020.** 13 types d'attaques par e-mail à connaître immédiatement. *Barracuda*. [En ligne] Mai 2020. [Consulté le 22 mars 2022.] https://assets.barracuda.com/assets/docs/dms/eBook_email-threats_fr-FR.pdf.

[129] **Barracuda. 2022.** Malware. [En ligne] 2022. [Consulté le 21 mars 2022.] https://fr.barracuda.com/glossary/malware#section_3.

3.2.7. Déploiement des CSIRT régionaux en France

« Les CSIRT régionaux apportent une réponse concrète et immédiate aux victimes de cyberattaques de taille intermédiaire partout sur le territoire national.

Concrètement, grâce au programme d'incubation, ces CSIRT régionaux seront en capacité de proposer très rapidement une aide personnalisée à la prise en charge des victimes, en les accompagnant depuis la déclaration de l'incident jusqu'à la fin de la remédiation, et en les orientant vers les bons prestataires et les bonnes actions à mener.

C'est une formidable occasion de proposer, aux entités des territoires, une réponse de proximité adaptée. » Guillaume Poupard, directeur général de l'ANSSI.

Un CSIRT (*Computer Security Incident Response Team)* est une équipe composée d'experts dévolue à la sécurité opérationnelle[130]. Ses principales missions sont les suivantes :

- Assurer une veille constante et maintenir une base de données récoltant les informations utiles sur les nouveaux enjeux, les nouvelles menaces, les dernières vulnérabilités recensées, etc… afin de mettre à jour sa connaissance de l'environnement cyber et appliquer les bons gestes au sein de son organisation.
- Jouer un rôle de prévention auprès de tous les utilisateurs ayant accès au SI de l'organisation en sensibilisant sur les bonnes pratiques, les principales menaces et leurs conséquences.
- Agir lors d'une crise cyber afin d'analyser et de traiter l'incident, dans le but de le résoudre.
- Bien qu'agissant pour le compte de son organisation, le CSIRT maintient un contact régulier avec d'autres acteurs pour assurer une plus grande coordination et une meilleure réponse face à un groupe d'attaquants : centres de compétence réseaux, opérateurs et fournisseurs d'accès à Internet, CSIRT nationaux et internationaux.

L'InterCERT France est une association loi 1901 qui constitue la première communauté de CSIRT en France. Elle est composée d'une soixantaine de sociétés publiques ou privées[131]. Ainsi, dans sa volonté de densifier les capacités françaises de réponse aux incidents cyber, l'ANSSI travaille aussi pour accompagner les TPE / PME / ETI dans leurs défenses cyber. Pour ce faire, des CSIRT régionaux sont en cours d'implantation afin de disposer d'un maillage national : 7 régions disposent d'un CSIRT régional en 2021 et font figure de pionniers[132]. L'objectif affiché est que chaque région dispose dès 2022 d'un tel centre et qu'il soit pleinement opérationnel au profit de tous les acteurs régionaux (collectivités, PME, ETI) au plus tard fin 2024.

[130] **CAPRONI, Nicolas. 2013.** Un CSIRT, à quoi ça CERT ? *CYBER-SECURITE.* [En ligne] 13 décembre 2013. [Consulté le 15 avril 2022.] https://www.cyber-securite.fr/2013/12/13/un-csirt-a-quoi-ca-cert/.

[131] **CERT-FR. 2022.** INTERCERT FRANCE. *CERT-FR.* [En ligne] 2022. [Consulté le 15 avril 2022.] https://www.cert.ssi.gouv.fr/csirt/intercert-fr/.

[132] **InCyber. 2022.** France : l'ANSSI créé sept CSIRT régionaux. *inCyber.* [En ligne] 12 janvier 2022. [Citation : 29 avril 2022.] https://incyber.org/france-anssi-cree-sept-csirt-regionaux/.

3.2.8. Espionnage industriel

Les exemples de vols d'informations sont nombreux et personne ne peut se considérer à l'abri de tels pillages, même les ETI. Les vols peuvent se faire physiquement, via le vol d'un ordinateur, effraction dans une chambre d'hôtel ou écoute de discussions lors d'un évènement professionnel. Cependant, les techniques d'espionnage industriel évoluent et deviennent plus techniques et immatérielles[133].

Les attaques subies par les entreprises privées ou publiques sont perpétrées à des fins d'extorsion mais aussi à des fins d'espionnage économiques ou scientifiques[134]. Dans le cas d'une attaque par rançongiciel ayant pour objectif de chiffrer les données et récupérer une rançon, l'attaquant n'a pas intérêt à s'attarder sur le système d'information de sa victime. Dans le cas de l'espionnage, l'attaquant va rechercher le maintien de ses accès aussi discrètement et longtemps possible afin de capter l'information stratégique. L'affaire des courriels d'Hillary Clinton en est un parfait exemple : des pirates informatiques ont infiltré en 2016 les serveurs du parti démocrate américain afin d'obtenir un maximum de données stratégiques et ce, pendant des mois[135].

En effet, il faut parfois des années à une organisation pour s'apercevoir de l'intrusion d'attaquant sur son SI ou qu'elle a été victime d'espionnage. L'attaquant, s'il sait rester discret et si l'entreprise néglige les règles d'hygiène informatique, peut rester silencieux et mettre la main sur les informations qu'il convoite. Le délai entre une intrusion et sa détection diminue : elle était en moyenne de 175 jours en 2017[136] et de 94 jours 2020 [137] . Souvent, lorsque les attaquants sont repérés, c'est parce qu'ils ont déployé un rançongiciels[138].

3.2.8.1. Captation et exfiltration d'informations via des attaques informatiques

L'attaque de l'homme du milieu (ou Man In The Middle - MITM) est une attaque lors de laquelle un tiers intercepte les communications entre deux systèmes, sans que leurs utilisateurs ne s'en aperçoivent[139].

Ce qu'il faut retenir, c'est que l'attaquant fait tout pour maintenir la connexion entre les systèmes informatiques. Il peut remplacer les éléments interceptés par d'autres (manipulation) ou simplement les écouter et les capter (espionnage).

---

[133] **PwC France. 2021.** Espionnage industriel - Une menace à appréhender avec détermination. [En ligne] 2021. [Consulté le 19 avril 2022.] https://www.pwc.fr/fr/decryptages/securite/espionnage-industriel-menace-a-apprehender-avec-determination.html.

[134] **ANSSI.** Une attaque réussie : combien de marchés potentiels perdus ? *ssi.gouv*. [En ligne] [Citation : 19 avril 2022.] https://www.ssi.gouv.fr/entreprise/principales-menaces/espionnage/.

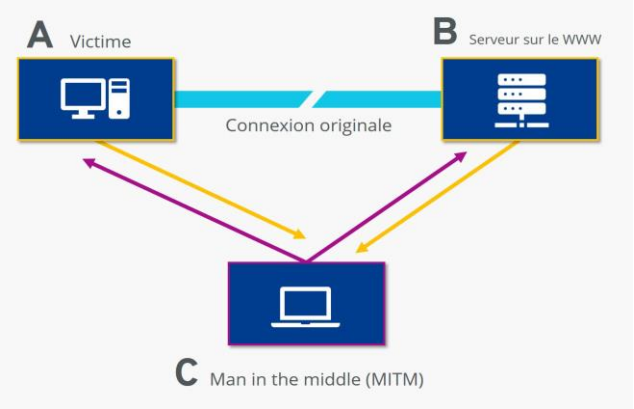
[135] **Ouest-France. 2018.** Comment les Russes ont espionné l'équipe Clinton, et chamboulé la présidentielle américaine. *Ouest-France*. [En ligne] 13 juillet 2018. [Citation : 19 avril 2022.] https://www.ouest-france.fr/monde/états-unis/comment-les-russes-ont-espionne-l-equipe-clinton-et-chamboule-la-presidentielle-americaine-5879669.

[136] **BEKY, Ariane. 2021.** Sécurité : 175 jours pour détecter une cyberattaque en Europe. *Silicon*. [En ligne] 2 mars 2021. [Citation : 20 avril 2022.] https://www.silicon.fr/securite-175-jours-detecter-cyberattaque-europe-205461.html#.

[137] **CHANDEZE, Aurélie. 2020.** Entre 3 et 7 semaines pour se rétablir après une cyberattaque. *CIO*. [En ligne] 12 novembre 2020. [Citation : 19 avril 2022.] https://www.cio-online.com/actualites/lire-entre-3-et-7-semaines-pour-se-retablir-apres-une-cyberattaque-12683.html.

[138] **TUNG, Liam. 2021.** Voici pendant combien de temps les attaquants se dissimulent dans votre réseau avant de déployer un ransomware ou d'être repérés. *ZDNet*. [En ligne] 20 mai 2021. [Citation : 20 avril 2022.] https://www.zdnet.fr/actualites/voici-pendant-combien-de-temps-les-hackers-se-dissimulent-dans-votre-reseau-avant-de-deployer-un-ransomware-ou-d-etre-reperes-39923061.htm.

[139] **C-Risk. 2021.** What is a MITM attack and how can you protect yourself against it? [En ligne] 10 septembre 2021. [Citation : 28 avril 2022.] https://www.c-risk.com/en/blog/mitm-attack/.



Représentation schématique d'une attaque de l'homme du milieu : le système C s'immisce en passant inaperçu dans la communication entre les systèmes A et B[140].

Pour infiltrer le trafic de données entre deux ou plusieurs systèmes, les hackers utilisent diverses techniques qui sont basées sur les vulnérabilités connues de la communication Internet.

Mais ils peuvent aussi se faire passer pour des points Wifi (Hotspots), on appelle ce schémas le jumeau maléfique (Evil Twin). Les attaquants mettent en place des points d'accès jumeaux maléfiques dans certaines zones comme un café, un hôtel, une gare, un parc (toute zone généralement desservie par le Wi-Fi gratuit ou public). La portée peut atteindre plusieurs entre 20 et 50 mètres s'il n'y a aucun obstacle gênant comme un mur en béton en cas d'attaque en intérieur[141].

Pour se protéger d'une attaque de l'homme du milieu, plusieurs solutions :

- S'assurer que les sites Web visités disposent de certificats d'authenticité, du protocole HTTPS et de l'icône du cadenas dans leurs URL.
- Éviter à tout prix d'utiliser les réseaux Wifi publics et préférer une connexion par accès mobile.
- Utiliser un VPN correctement configuré pour que le chiffrement et ainsi la protection des données entre les deux participants soient assurés de bout en bout (sur le poste de travail et les téléphones mobiles des salariés).
- Utiliser un antivirus sur les téléphones mobiles des salariés.

Le reniflage (sniffing) est une autre technique permettant d'analyser un trafic réseau. L'utilisation d'un programme installé sur une machine mettant en évidence les trames qui passent par sur un réseau peut être tout à fait légitime et utilisé par les services informatiques pour analyser un problème réseau ou superviser un trafic. Cependant, un logiciel avec un tel potentiel d'espionnage peut être dangereux s'il est utilisé à des fins malveillantes comme la récupération d'emails, de mots de passe, ou de paquets contenant des données confidentielles non chiffrées. Là encore, le maintien d'un renifleur peut durer des années. Les renifleurs malveillants sont souvent installés par d'autres logiciels malveillants tels que des virus ou des chevaux de Troie. Pour s'en protéger, il est conseillé d'utiliser des protocoles de communication chiffrés (SSH et SSL) et de mettre en place un détecteur de renifleur[142].

[140] **IONOS. 2019.** Attaque Man in the Middle (MITM). [En ligne] 19 mars 2019. [Citation : 28 avril 2022.] https://www.ionos.fr/digitalguide/serveur/securite/attaque-de-lhomme-du-milieu-apercu-du-modele/.

[141] **Blackbird. 2020.** Black Wifi : l'exemple d'un faux point d'accès. *Les dossiers du Pirate*. SARL ID Presse, octobre - décembre 2020, N°25, pp. 52-53.

[142] **Oracle. 2020.** Qu'est-ce qu'un sniffer ? *Oracle*. [En ligne] 2020. [Citation : 28 avril 2022.] https://www.oracle.com/fr/security/definition-sniffer-renifleur.html.

Les données sensibles comme des identifiants et des mots de passe peuvent aussi être captées via un enregistreur de touches (ou Keylogger). Il s'agit d'un logiciel espion (ou un boîtier, facilement détectable) capable d'enregistrer les frappes sur le clavier d'un ordinateur.

3.2.8.2. Captation et exfiltration d'informations via des attaques physiques

Des mesures de sécurité physique doivent être mises en place afin de protéger l'accès aux bâtiments, l'équipement, les données et les salariés. En bref, ils empêchent les personnes non autorisées d'entrer de manière frauduleuse et de mettre en péril la sécurité de l'entreprise. En complément de la sécurité logique et des contrôles informatiques voués à sécuriser le réseau et l'infrastructure, la sécurité physique permet de protéger l'entreprise contre le vol, le vandalisme, la fraude, les accidents et l'impact des catastrophes naturelles[143]. Un plan de sécurité physique complet combine la technologie et le matériel spécialisé, et doit inclure des contre-mesures contre les intrusions telles que :

- La conception et aménagement du site.
- Les composants environnementaux.
- La sensibilisation et la préparation aux interventions d'urgence.
- Les contrôles d'accès.
- La détection des intrusions.

Les stratégies de sécurité les plus élaborées adoptent une approche superposant les contrôles de sécurité physique et une politique de cybersécurité. Les quatre principales composantes de la sécurité physique sont[144] :

1. Dissuasion – Il s'agit des mesures de sécurité physique qui empêchent les personnes d'entrer ou qui les forcent à s'éloigner des locaux. Les composants de sécurité dissuasifs peuvent être une barrière physique, telle qu'un mur, une porte, un grillage ou un tourniquet. La technologie peut également être dans cette catégorie. Les systèmes de contrôle d'accès, le verrouillage à distance et les caméras de sécurité vidéo dissuadent également les personnes non autorisées de tenter d'accéder au bâtiment.

2. Détection - Les composants de détection de votre système de sécurité physique aident à identifier un événement de sécurité potentiel ou un intrus. Les capteurs, les alarmes et les notifications automatiques et des agents de sécurité (aussi utiles comme outil de dissuasion) sont tous des exemples de détection de sécurité physique.

3. Atténuation - Certains systèmes de sécurité sont conçus pour ralentir les intrus lorsqu'ils tentent d'entrer ou sont entrés dans une installation ou un bâtiment. Le contrôle d'accès, tel que l'exigence d'une carte-clé, des identifiants, les multi-factor authentication (MFA) est une méthode d'atténuation.

---

[143] **Département TI. 2020 .** Les aspects de sécurité d'un centre de données. *Département TI*. [En ligne] 2020 . [Citation : 28 avril 2022.] https://www.departement-ti.com/2019/11/18/les-aspects-de-securite-dun-centre-de-donnees/.

[144] **Openpath. 2020.** Guide to Physical Security in the Workplace. *Openpath*. [En ligne] 2020. [Citation : 09 mai 2022.] https://info.openpath.com/hubfs/Openpath-Physical-Security-Guide.pdf?utm_medium=email&_hsmi=97869752&_hsenc=p2ANqtz-9HZkUjNFJozp3gnkh2XUCbpNGsgxpMqPwky28wFzkdy3xhO28VNgiecOluEbb-qibjwc-9GBMgVxuRUo5c468cPq_EtQ&utm_content=97869752&utm_source=hs_automation.

4. Réponse - Ce sont les composants qui sont en place une fois qu'une violation ou une intrusion se produit. Les exemples d'intervention de sécurité physique comprennent les systèmes de communication, le verrouillage des bâtiments et la prise de contact avec les services d'urgence ou une équipe sur place.

En complément, les actions suivantes peuvent être envisagées pour construire et maintenir un environnement de sécurité acceptable. :

- Restreindre l'accès aux locaux et plus spécifiquement les salles informatiques hébergeant les serveurs, les locaux contenant des données papier sensibles (comptabilité, client, R&D…) et partout où les ordinateurs sont laissés sans surveillance.
- Recourir à une équipe et des outils de sécurité vérifiant que chaque salarié est autorisé à pénétrer dans les locaux, empêchant ainsi le talonnage[145] (lorsqu'un ou plusieurs individus suivent une personne autorisée à travers un accès sécurisé), l'agglutinement (deux individus essayant de se coller pour n'en paraître qu'un).
- Accompagner à tout moment les visiteurs et s'assurer qu'ils ont un badge « visiteur » visible.
- Utilisez des informations d'identification d'accès hautement sécurisées, difficiles à cloner, entièrement traçables et uniques à chaque individu.
- Exiger une authentification multifacteur (MFA) pour déverrouiller une porte ou accéder au bâtiment.
- Structurer les autorisations pour utiliser l'accès au moindre privilège dans l'ensemble de l'infrastructure physique.
- Éliminer les redondances entre les équipes et les processus pour une réponse plus rapide aux incidents.
- Configurer des alertes de sécurité automatisées pour surveiller et identifier les activités suspectes en temps réel.
- Éviter d'utiliser les ordinateurs portables (ou fournir à minima des filtres de confidentialité sur les écrans) et de consulter des documents confidentiels dans des lieux publics comme une gare ou un train afin d'éviter le shoulder surfing (espionnage visuel direct ou enregistrement vidéo)[146].
- Éviter de branchement de clés USB visant à répandre un malware (rubber ducky) ou extraire des données.

[145] **MORTON, Jennie. 2011.** 10 strategies prevent tailgating. *Buildings*. [En ligne] 06 décembre 2011. [Citation : 08 mai 2022.] https://www.buildings.com/articles/31764/10-strategies-prevent-tailgating.

[146] **IONOS. 2020.** Shoulder surfing – un danger sous-estimé ? *IONOS*. [En ligne] 14 septembre 2020. [Citation : 08 mai 2022.] https://www.ionos.fr/digitalguide/serveur/securite/shoulder-surfing/#:~:text=Le%20shoulder%20surfing%20fait%20partie,donn%C3%A9es%20par%20une%20observation%20directe.

3.2.8.3. Les contrôles généraux informatiques comme outil d'hygiène et de discipline informatique

Indépendamment des outils sur lesquels une entreprise peut s'appuyer pour optimiser sa maîtrise des risques, il existe les 3 lignes de défense[147] :

1. Le business est responsable de la détection des risques dans son domaine d'activité et de la mise en place de contrôles efficaces.
2. Les fonctions Risques, Compliance et, pour certains aspects, Affaires financières, juridiques et fiscales et Protection du risque de l'information. Indépendantes du business, les fonctions de contrôle et de risque de deuxième ligne formulent leur avis concernant les risques auxquels l'entité est confrontée.
3. Audit interne. En tant que contrôle de troisième ligne indépendant, l'Audit interne est responsable du contrôle de qualité des processus d'entreprise existants.

La deuxième ligne de défense incarne la fonction de contrôle interne qui est défini par l'Institut Français de l'Audit et du Contrôle Interne comme « un processus continu mis en œuvre par le conseil, le management et les collaborateurs d'une entité, destiné à fournir une assurance raisonnable quant à la réalisation d'objectifs liés aux opérations, au reporting et à la conformité »[148].

Ainsi, une série de contrôles peuvent être réalisés en continu (certains périodiquement) sur tous les tiers du SI (application, base de données, serveurs) et peuvent permettre de diminuer le risque d'une intrusion, voire d'en détecter. Voici une liste non exhaustive de contrôles préventifs et détectifs issus du référentiel COSO (Committee Of Sponsoring Organizations) :

- Chaque création ou modification d'un accès utilisateur se doit d'être réalisée et validée par 2 personnes.
- Tout accès au SI se doit d'être désactivé dans un délai raisonnable en cas de départ d'un utilisateur ou d'une mutation.
    - Départ : certains comptes sont maintenus par les collègues car les droits octroyés à l'utilisateur ayant quitté les effectifs rendent les processus métier « plus simples », mais bien entendu aussi plus risqués.
    - Mutation : Au gré des années, certains utilisateurs ont des droits extrêmement larges car leurs accès n'ont jamais été adapté à leur nouveau poste.
- Au moins une fois par an, le management doit réaliser la revue des comptes actifs du SI :
    - Quantitativement : désactiver tous les comptes actifs n'ayant pas été captés par le contrôle de désactivation au fil de l'eau.
    - Qualitativement : chaque compte doit avoir ses droits / profils confirmés et recertifiés afin de s'assurer que ceux-ci sont en adéquation avec les besoins et les rôles de l'utilisateur.

[147] **IFACI et AMRAE. 2013.** Trois lignes de maîtrise pour une meilleure performance. *IFACI*. [En ligne] 2013. [Citation : 06 mai 2022.] https://docs.ifaci.com/wp-content/uploads/2018/03/Trois_lignes_de_ma%C3%AEtrise_pour_une_meilleure_performance.pdf.

[148] **IFACI. 2013.** LES MÉTIERS DE L'AUDIT ET DU CONTRÔLE INTERNES. *IFACI*. [En ligne] 2013. [Citation : 06 mai 2022.] https://www.ifaci.com/audit-controle-interne/metiers-de-laudit-controle-internes/#:~:text=Le%20contr%C3%B4le%20interne%20est%20un,reporting%20et%20%C3%A0%20la%20conformit%C3%A9..

- Identifier les actions les plus critiques réalisées par les utilisateurs métiers, les administrateurs (applicatifs et sur les couches basses) et les comptes génériques partagés afin de les tracer et les revoir de manière périodique. Ainsi, toute activité suspecte serait identifiée (connexion à des heures indues, utilisation d'un compte générique qui n'est jamais utilisé par l'équipe IT…).

- Limiter au maximum l'utilisation de comptes génériques (perte de la traçabilité de qui agit sur ce compte), administrateurs et à droits étendus. Cette pratique est très répandue au sein des DSI : les administrateurs de base de données se connectent tous sur le même compte administrateurs, souvent le compte d'initialisation dont le mot de passe initial n'a jamais été modifié.

- S'assurer que chaque utilisateur ne dispose que d'un compte par application. La multiplicité des comptes actifs pour le même utilisateur permet de contourner la séparation des tâches mise en place au sein d'une application.

- S'assurer que les mots de passe initiaux des comptes d'installation sont modifiés. S'assurer de l'application d'une politique de sécurité et de mot de passe en ligne avec les recommandations de l'ANSSI et de l'ISACA.

- Au niveau des projets informatiques, documenter le processus d'évolution et de mise en production, via des tickets, des cahiers de tests, des bons pour mise en production.

- S'assurer de la séparation des tâches entre les différents environnements : éviter que les développeurs n'aient accès à la production et puissent réaliser eux même les mises en production. Cela induit un risque développement et déploiement de modification non autorisée.

- Avoir un PCA / PRA en place testé et mis à jour régulièrement.

- Mettre en place une politique de sauvegarde et réaliser des tests de restauration.

- Mettre en place des contrôles automatiques bloquants afin que tout processus ne puisse pas être suivi de bout en bout par une seule et même personne.

3.2.8.4. Les coûts des fuites de données

Fort des réponses obtenues lors de ses recherches, le Ponemon Institute a pu dégager les principaux coûts (internes et externes) liés à une fuite de données.

a. Coûts d'origine externes

Le coût de la perte ou du vol d'une information comme les données sensibles et/ou confidentielles comme les secrets d'affaires, les propriétés intellectuelles, les données clients, le code source d'un logiciel est bien évidemment important. Il faut aussi y ajouter le prix que l'entreprise devra payer pour la notification de cet incident de sécurité (obligatoire s'il s'agit d'une fuite d'information liée aux données personnelles sous peine d'amende de la part de la CNIL)[149]. Le vol d'information de connexion (identifiant / mot de passe) est de loin la menace la plus coûteuse à remédier du fait de l'impact que peut constituer des accès non autorisés à un système d'information dans le but de nuire.

Le coût d'une interruption d'activité comprend les impacts des temps d'arrêt, des retards ou même des pannes imprévues qui peuvent déstabiliser l'organisation.

[149] **CYBERARK. 2019.** Fuite de données. [En ligne] 2019. [Citation : 04 mai 2022.] https://www.cyberark.com/fr/what-is/data-breach/.

Le coût lié à l'impact sur le chiffre d'affaires suite à la perte de clients, de prospects et même de partenaires, du fait de retards ou d'annulation de projets. Ce coût comprend aussi la perte de confiance perçue par les partenaires suite à la divulgation d'une attaque.

b. Coûts internes

Monitoring et surveillance
- Activités de détection, de prévision et de dissuasion des incidents.

Investigation
- Activités nécessaires pour identifier la cause, la source, les parties prenantes, l'ampleur et les impacts de l'incident.

Escalade
- Activités permettant la communication interne à destination des parties prenantes concernées par l'incident.

Réponse aux incidents
- Activités permettant une réponse et une prise de décision rapide par les experts et la direction.

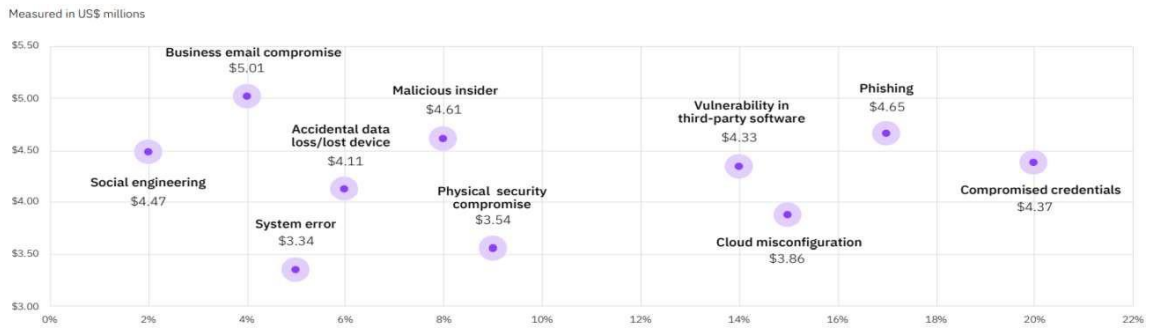
Confinement
- Activités qui permettent de réduire la gravité des incidents ou des attaques internes (notamment via la fermeture des applications et des terminaux vulnérables).

Retours d'expérience
- Activités permettant de formaliser les informations qui aideront l'entreprise à empêcher ou minimiser les futurs incidents et attaques internes.

Actions correctives / remédiations
- Activités liées à l'application de correctifs / mises à jour / remplacements des équipements et des différents actifs informatiques à la suite d'attaques internes contre les systèmes d'information et les infrastructures critiques

Il faut savoir que l'investissement engagé dans les contrôles préventifs est toujours rentabilisé. En effet, 56 % des PME qui subissent un préjudice oscillant entre 10 000 et 100 000 € voient leur activité mise en danger du fait de la fragilisation de leur trésorerie[150].

Une étude réalisée par IBM Security et Ponemon Institute en 2021 ont démontré que le coût moyen d'une fuite de données en France est de 4,42 millions de dollars. Certains facteurs comme le zero trust, les contrôles de sécurité automatisés et la mise en place d'un cloud hybride permettent de mitiger les risques et le coût d'une fuite de données. La fréquence et le coût d'une fuite de donnée est hétérogène selon le vecteur d'attaque :



Coût total moyen et fréquence de fuite de données par vecteur d'attaque [151]

[150] **NAGEOTTE, Agathe. 2021.** Données sensibles des entreprises : comment les sécuriser ? *oodrive*. [En ligne] 19 avril 2021. [Citation : 04 mai 2022.] https://www.oodrive.com/fr/blog/securite/donnees-sensibles-entreprise/#:~:text=Pour%20se%20prot%C3%A9ger%2C%20il%20est,confidentialit%C3%A9%20des%20%C3%A9changes%20est%20essentielle..

[151] **Security, IBM. juillet 2021.** *Cost of a data breach report*. New York : s.n., juillet 2021.

À mesure que le volume et le temps nécessaires pour contenir les menaces internes augmentent, les technologies avancées telles que les outils de comportement des utilisateurs et l'automatisation sont importantes pour aider à réduire les menaces internes. Des outils basés sur le comportement des utilisateurs, le User Behavior analytics[152] (ex : Splunk) pour détecter les menaces internes sont considérés comme très importants pour réduire les menaces internes pour 62 % des répondants. Il faut aussi considérer l'automatisation pour la prévention, l'investigation, l'escalade, le confinement et la résolution des incidents internes comme le Data Loss Prevention [153] (ex : Forcepoint ou Proofpoint) ou encore l'utilisation d'outils de scan automatique du web (darknet compris) afin d'identifier des données qui auraient fuité (ex : CybelAngel)[154].

3.2.9. La désinformation opérationnelle[155]

A la frontière entre le défensif et l'offensif, la désinformation opérationnelle peut être classée dans la catégorie de la « défense active ».

Avant de découvrir la partie dédiée à l'aspect offensif et dissuasif de la guerre de l'information, intéressons-nous à la manière dont la ruse peut permettre à une entreprise d'éviter les attaques et de se jouer de ses concurrents prédateurs.

Afin de supplanter ses concurrents, la ruse doit souvent faire partie du mode opératoire d'une entreprise. A l'instar d'un conflit militaire, la force pure ne suffit pas, surtout lorsqu'on se place du côté de David face à Goliath. Dans ce domaine pointu qu'est la ruse, la désinformation occupe une place capitale. Cette action fallacieuse consiste à répandre des informations déformées afin de manipuler l'imaginaire collectif ou les décideurs concurrents (dans le privé comme le public). Dans le domaine militaire, on parle de désinformation opérationnelle.

Elle vise à induire un ennemi en erreur pour lui faire adopter une attitude inadéquate qui facilitera la manœuvre amie. Comme pour de nombreux autres sujets, ce qui est valable dans le champ militaire l'est dans le champ économique : 3 techniques ont été largement éprouvées (simulation, imitation, intoxication). L'important reste de toujours rester dans le domaine du légal, et induire des concurrents en erreur afin de gagner un avantage compétitif ne doit pas représenter une quelconque concurrence déloyale ou violation de la loi.

---

[152] **Rapid7. 2019.** What is user and entity behavior analytics? (UEBA). *Rapid7*. [En ligne] 2019. [Citation : 27 avril 2022.] https://www.rapid7.com/fundamentals/user-behavior-analytics/.

[153] **Proofpoint. 2021.** Qu'est-ce que la Data Loss Prevention (DLP) ? *proofpoint*. [En ligne] 2021. [Citation : 23 mai 2022.] https://www.proofpoint.com/fr/threat-reference/dlp.

[154] **LAMIGEON, Vincent. 2021.** CybelAngel, la pépite cyber française, entre au Next40. *Challenges*. [En ligne] 08 février 2021. [Citation : 03 mai 2022.] https://www.challenges.fr/entreprise/cybelangel-la-pepite-cyber-francaise-entre-au-next40_750002.

[155] **KLEN, Michel. 2020.** La désinformation opérationnelle. *Cairn.info*. [En ligne] 17 février 2020. [Citation : 15 avril 2022.] cairn.info/revue-defense-nationale-2016-1-page-114.htm?contenu=resume.

3.2.9.1. Simulation : l'exemple de l'obfuscation

La simulation est l'accomplissement d'activités destinées à masquer les préparatifs d'une opération et à leurrer l'adversaire sur le lieu exact d'une attaque. Nous pouvons penser à l'obfuscation, une méthode de protection de l'information qui vise à en obscurcir sa précision[156]. Cette méthode peut être définie comme «la création délibérée d'informations surabondantes, ambiguës, désordonnées ou fallacieuses en les mélangeant aux données véridiques afin de rendre plus difficiles leur collecte, leur analyse et leur utilisation »[157]. Ainsi, tout ce qui peut brouiller, opacifier, masquer, noyer, rendre illisible les informations est un mode d'obfuscation. Les informations seront mieux protégées car plus difficiles d'accès et moins intelligibles au milieu d'autres informations moins pertinentes. Etant donné que les informations sont aujourd'hui presque impossibles à supprimer sur internet (en raison des la rapidité de diffusion et du caractère mondialisé des systèmes d'information), il peut être judicieux de publier un grande quantité d'informations, parfois fausses, imprécises ou non-pertinentes afin de noyer les données à protéger dans un grand volume de données.

Cette technique rappelle le premier des 36 stratagèmes, l'ensemble des principes stratégiques applicables dans l'art de la guerre, de la politique, de la diplomatie ou des tractations commerciales. Ce stratagème s'intitule : « En dupant le ciel, traverser la mer ». En effet, notre esprit critique est éveillé par ce qui est inhabituel. Afin de détourner l'attention d'un adversaire, il faut déployer sa stratégie dans des actions banales. Cela est applicable pour la gestion de ses données : agir de manière banale pour cacher une avancée dans un projet de recherche et développement, ou inonder l'adversaire de données d'apparence dépourvues d'intérêt pour se protéger.

Parmi toutes les techniques de protection de ses données, trois sont particulièrement utilisées[158] :

- **Le chiffrement :** permet de sécuriser toutes vos données. Utiliser un protocole de chiffrement connu comme étant plus sécurisé pourrait attirer des soupçons (ou justement utiliser un protocole particulièrement sécurisé pour des données sans intérêt, pour susciter l'intérêt et détourner des données vraiment sensibles).

- **La tokenisation :** remplace les données sensibles par une valeur qui n'a pas de sens. Bien que ce processus ne puisse pas être inversé, il est possible de mapper le jeton sur les données d'origine

- **Le masquage des données :** ce processus, aussi appelé brassage, aveuglement ou brouillage, remplace les données originales par des données réalistes mais fausses pour garantir la confidentialité. En utilisant des données masquées, les équipes de test, de formation, de développement ou d'assistance peuvent travailler avec un ensemble de données sans mettre en danger les données réelles.

[156] **L'internaute. 2021.** Obfuscation. *l'internaute.* [En ligne] 01 janvier 2021. [Citation : 13 mai 2022.] https://www.linternaute.fr/dictionnaire/fr/definition/obfuscation/#:~:text=L'obfuscation%20consiste%20%C3%A0%20prot%C3%A9ger,suppression%20de%20donn%C3%A9es%20trop%20personnelles..

[157] **DELAHAYE, Jean-Paul. 2019.** L'offuscation ou l'art de brouiller l'écoute. *Pour La Science.* [En ligne] 29 octobre 2019. [Citation : 30 mars 2022.] https://www.pourlascience.fr/sr/logique-calcul/l-offuscation-ou-l-art-de-brouiller-l-ecoute-18265.php.

[158] **Talend. 2022.** What is Data Obfuscation? *Talend.* [En ligne] 2022. [Citation : 28 mars 2022.] https://www.talend.com/resources/data-obfuscation/.

3.2.9.2. Imitation : l'exemple des Honeypots et des Honeynets

L'imitation consiste à reconstituer des éléments fictifs pour abuser des moyens de reconnaissance adverses. À titre de mesure préventive ou de défense active, une entreprise peut mettre en place un ensemble de serveurs ou de systèmes volontairement vulnérables. Une fois le piège posé, l'objectif consiste à attendre l'intrusion d'attaquants, pensant tirer profit du manque de précautions de sa victime. Le honeypot n'est pas à proprement parlé voué à attaquer l'attaquant en justice mais à le ralentir, le rendre confus et en apprendre plus sur les schémas d'attaque et les motivations. Plus crédible, un honeynet est un réseau de honeypots interconnectés qui simule un véritable réseau, plus hétérogène, comme le serait un véritable système d'information. Le honeypot peut être physique (ordinateur autonome connecté à un réseau) ou virtuel (système logique sur lequel tourne un logiciel de virtualisation). Ils peuvent être côté serveur, en attirant les attaquants dans des zones isolées de système d'information en vue d'en apprendre plus, ou côté client, en imitant un logiciel d'application[159].

Attention, un honeypot est un outil qui doit être utilisé en complément d'autres composants indispensables de la sécurité informatique, comme des antivirus, des pare-feu et potentiellement des systèmes de détection d'intrusion (IDS). Une séparation maximale entre la production (les systèmes « légitimes ») et le honeypot doit être maintenue et aucune donnée de production ne doit être répliquée sur le système servant de leurre.

Les avantages d'un honeypot[160]:

- Apprendre : observer un attaquant naviguer sur le système d'information mis à sa disposition peut être riche d'apprentissage. En effet, il est alors possible de connaître ses modes opératoires, les outils qu'il utilise et ses motivations. En analysant son comportement, on peut aussi, potentiellement, découvrir s'il est en possession de connaissances sur l'entreprise acquise par ingénierie sociale, un piratage antérieur, ou provenant d'une personne interne.

- S'améliorer : la phase d'observation et d'analyse peut aider le service sécurité à mettre l'accent sur certaines techniques de défense et des mises à jour logicielles à passer en priorité. Idem pour des erreurs de paramétrages qui peuvent être mises en lumière par les tentatives d'intrusion de l'attaquant.

- Former : le honeypot et le honeynet sont des outils pédagogiques notamment pour les entreprises dont le code de déontologie défend de recourir à des hackers pour sécuriser leur système d'information et qui manquent dont de connaissances sur les schémas d'attaque. Ils permettent d'être mieux préparés à gérer une crise cyber et à mener des investigations. Ces outils sont encore peu utilisés en France, contrairement aux États-Unis, mais le marché devrait continuer à s'ouvrir.

Les inconvénients d'un honeypot :

- Parfois peu efficace : un honeypot ne fournit pas toujours des informations exploitables. Si l'appât est trop peu attractif, trop évident ou trop difficile à atteindre, le risque est de n'avoir aucune attaque et donc un retour nul sur les investissements financiers et humains pour la mise en place de ce système de sécurité.

[159] **IONOS. 2017.** Honeypot - sécurité informatique via des leurres. *IONOS*. [En ligne] 08 août 2017. [Citation : 04 mai 2022.] https://www.ionos.fr/digitalguide/serveur/securite/honeypot-securite-informatique-via-des-leurres/.

[160] **SCHNEIDER, Bruce. 2001.** Secrets et mensonges - Sécurité numérique dans un monde en réseau. [En ligne] 2001. [Citation : 07 mai 2022.] http://strategique.free.fr/archives/textes/hacking/archives_hacking_13.htm.

- Coûteux : il s'agit d'un outil dont la mise en place est coûteuse car même s'il est possible de recycler de vieilles machines, l'expertise technique du prestataire de services a un coût.

- N'empêche pas forcément une intrusion : bien que le Honeypot fasse fonction de diversion, il existe toujours même un risque que les causent des dégâts sur le réseau lors d'une intrusion.

3.2.9.3. Intoxication : les exemples des brevets et des noms de domaines

L'intoxication vise à injecter chez l'adversaire des nouvelles erronées pour fausser le jugement. Cela fait écho au 6ème des 36 stratagèmes : « faire du vacarme à l'est pour attaquer à l'ouest ». L'utilisation de l'intoxication pourra servir les pratiques de diversion. Prenons l'exemple des brevets et des noms de domaines.

Faux brevet : bien souvent, le dilemme est de déposer un brevet (afin de protéger une propriété intellectuelle mais en la dévoilant au monde) ou cultiver le secret (et ainsi être à risque d'espionnage). Michelin, très souvent pris en exemple pour sa gestion de sa R&D entre secret et brevets. Jacques Bauvir, Chef du Service Propriété Intellectuelle de Michelin déclare : « notre principe de base est de breveter tout ce qui se voit et de garder secret ce qui peut l'être, notamment ce qui concerne la fabrication »[161].

Ainsi peut-il être intéressant de breveter la propriété intellectuelle qui ne représente pas une priorité absolue pour l'entreprise, afin que les concurrents se fourvoient en pensant qu'il s'agit du résultat des recherches les plus poussées de l'entreprise (alors que les informations les plus précieuses restent protégées et secrètes). Sachant cela, la mise en place de la sécurité la plus stricte des données est de rigueur, afin que la propriété intellectuelle ne se perde pas, ne soit pas détruite ou volée.

DNS : Si une entreprise sait qu'un concurrent se renseigne sur ses activités, une stratégie d'intoxication pourrait consister en l'achat d'une extension de domaine étranger. Ainsi, le concurrent pourrait croire que l'entreprise surveillée souhaite développer son activité à l'étranger. Le concurrent va donc être induit en erreur, perdre du temps et des ressources à se renseigner sur les raisons et les signaux qui viendraient confirmer un développement de son activité sur un nouveau marché, voire de se détourner du marché ciblé par l'entreprise surveillée ayant piégé le concurrent.

[161] **INPI. 2014.** Secret(s) ou brevet(s) ? La réponse de Michelin. [En ligne] 2014. [Citation : 18 mai 2022.] https://www.inpi.fr/fr/valoriser-vos-actifs/le-magazine-de-la-valorisation/secrets-ou-brevets-la-reponse-de-michelin.

3.3. Aspects offensifs de la guerre de l'information

« Si vous connaissez vos ennemis et que vous vous connaissez vous-même, mille batailles ne pourront venir à bout de vous » - Sun Tzu, L'Art de la guerre

Cette partie du mémoire a pour objectif de porter à la connaissance des dirigeants de méthodes (non-exhaustives) employées aujourd'hui dans le cadre d'affrontements économiques entre acteurs.

Avant tout, les auteurs souhaitent sensibiliser et convaincre les dirigeants à appliquer une posture dissuasive (en complément de celle adressée sur le plan physique dans la partie « Espionnage industriel ») et offensive dans leurs entreprises pour éviter qu'elles ne soient impactées dans la compétition économique mondiale et nationale. Nous l'aborderons ici, au travers du prisme du renseignement (d'état et de sa transposition en renseignement économique).

En garde ! Êtes-vous prêts ? Allez ! Brisons nos tabous culturels Français et ripostons face à la datasphère.

La guerre de l'information adressée dans le cadre de la guerre économique est avant tout un état d'esprit. Alain Juillet[162], haut responsable chargé de l'intelligence économique au sein du SGDN[163] (Secrétariat Général de la Défense Nationale) entre 2003 et 2009, précisait qu'il fallait faire prendre conscience [ndlr aux entreprises] de l'importance du renseignement économique dans l'économie de la connaissance à l'heure où l'offre et la demande ne permettent plus de se créer un avantage concurrentiel durable [2008].

Depuis ces propos, et comme exposé dans le chapitre « Révolution technologique », le développement du volume de données n'a cessé de croître de manière exponentielle généré par les systèmes d'informations des entreprises de plus en plus interconnectés à Internet et nos usages numériques personnels.

Cette masse abyssale d'information accessible (c.f. paragraphe « les différents types d'information") est une mine de renseignements utile pour celui qui est en mesure de valoriser les informations.

Le « renseignement utile » ou renseignement économique résulte d'un processus d'activités issu de l'Intelligence économique[164].

Instaurer le renseignement économique au sein de son entreprise permettra au(x) dirigeant(s) d'accéder aux bonnes informations (en respectant les règles légales) pour se développer ; une pratique pleinement alignée avec une politique d'anticipation et d'innovation d'entreprise.

Pour ce faire, la plus haute autorité de l'entreprise doit inscrire la Fonction d'Intelligence Économique à ses côtés et prendre place au sein du Comité Exécutif.

[162] **JUILLET Alain, DAGUZAN Jean-François.** L'intelligence économique en question(s). Cairn.info/Sécurité globale 2008/4 (N° 6), p. 9-18. [En ligne] 01/10/2013. [Consulté en mai 2022.] DOI : 10.3917/secug.006.0009. URL : https://www.cairn.info/revue-securite-globale-2008-4-page-9.htm

[163] En 2009, le SGDN s'est transformé en un secrétariat général de la défense et de la sécurité nationale (SGDSN) doté de missions élargies (http://www.sgdsn.gouv.fr/)

[164] **Portail de l'IE.** Les définitions de l'intelligence économique. [En ligne] 19 janvier 2013. [Consulté en mai 2022] https://portail-ie.fr/les-definitions-de-lintelligence-economique

Par rapport à la veille - concept apparu dans les années 1980 - (c.f. partie « L'importance de la veille dans la guerre de l'information »), l'Intelligence Économique - introduite en France en 1992 - intègre des objectifs supplémentaires (non adressés ou partiellement dans ce mémoire) :

- La protection du patrimoine informationnel.
- La capacité d'influence et de notoriété.

3.3.1. L'Intelligence économique, l'alliée des dirigeants

Lors de la conférence « Sécurité économique et cybersécurité : un enjeu pour toutes les entreprises », organisée le 17 mars 2022 à Clermont-Ferrand, Julien Lopizzo, DG de Major Corp a souligné « qu'une fois qu'on pense qu'un événement est impossible, c'est l'improbable qui surgit ».

Pour faire face aux situations improbables, la production structurée d'informations décisionnelles pour la stratégie d'une entreprise et leur utilisation à des fins de protection, de développement ou d'influence revêt une importance capitale.

L'intelligence économique permet ainsi aux dirigeants d'anticiper les risques ou les opportunités et donc de s'y préparer comme exposé précédemment dans le mémoire.

Jérôme Bondu, expert en Intelligence Économique a lui l'habitude de la définir comme étant « le système immunitaire de l'entreprise »[165 et 166].

3.3.2. Justification d'adoption d'une posture de cyber-renseignement

Bien que non-exhaustives, les cas exposés ci-dessous illustrent les motifs d'instaurer une cellule interne ou externe de renseignement économique.

> « Défini(e) simplement, [l'inflation de la menace] est l'effort fait par les élites pour créer une préoccupation pour une menace qui va au-delà de la portée et de l'urgence qu'une analyse désintéressée pourrait justifier.
>
> Plus largement, le processus concerne la manière dont les élites perçoivent les menaces, leur utilisation politique, comment les politiques de réponses aux menaces interviennent dans la compétition politique entre les élites et la manière dont le public interprète et perçoit les menaces à travers les nouveaux médias » expliquent Jane Cramer et Trevor Thrall dans *American Foreign Policy and the Politics of Fear* [2009].

[165] **SAURY, Raphaëlle. BONDY, Jérôme ou la vision humaine de l'intelligence économique. 2001.** [En ligne] 21 décembre 2011. [Consulté en mai 2022] https://portail-ie.fr/short/198/jerome-bondu-ou-la-vision-humaine-de-lintelligence-economique

[166] **BONDU, Bondu. Rôle du consultant en intelligence économique. 2022.** [En ligne] 22 février 2022. [Consulté en mai 2022.] https://www.inter-ligere.fr/34metaphore-medicale-sur-l-intelligence-economique/

3.3.2.1. L'inflation de la menace

Comme décrit en début de document, les tensions internationales sont nombreuses en 2022 engendrées par des années de pandémie à la COVID-19, le dérèglement climatique, les déplacements de population, les conflits géopolitiques, les conflits armés, etc.

Ces tensions révèlent « de nouveaux besoins en termes de renseignement mais aussi la formalisation d'une « dissuasion informationnelle » qui ne se limite pas à la détection de la désinformation ou des *fake news*. A partir d'une détection précoce de la résonance des fausses informations, issue d'une combinaison de vecteurs différents, nous devons être en mesure de réagir tout aussi rapidement en rétablissant tout simplement les faits. » comme le révèlent Vincent Barbé et Olivier Laurent[167].

Ces menaces n'ont pas de frontière numérique tel que le souligne l'ANSSI dans un bulletin d'actualité : « Les tensions internationales actuelles causées par l'invasion de l'Ukraine par la Russie, s'accompagnent d'effets dans le cyberespace. Si les combats en Ukraine sont principalement conventionnels, l'ANSSI constate l'usage de cyberattaques dans le cadre du conflit. Dans un espace numérique sans frontières, ces cyberattaques peuvent affecter des entités françaises et il convient sans céder à la panique de l'anticiper et de s'y préparer. »[168]

L'une des mesures contre ces menaces est d'adopter une posture dissuasive qui « est destinée à la paralysie des actions offensives adverses par crainte de représailles supérieures à l'espoir de gain »[169].

3.3.2.2. La concurrence

Pour faire face au marché concurrentiel (évoqué à plusieurs reprises précédemment), le dirigeant doit mettre en place une stratégie à partir d'informations valorisées. Or, le renseignement engendre « Le dilemme de la sécurité ».

Transposons ici l'approche réaliste des relations internationales et de la sécurité entre deux pays concurrents développée par Robert Jervis dans son article « Cooperation under the Security Dilemma »[170] sur le plan économique. Supposons deux entreprises concurrentes, Industriel A et Industriel B ayant des relations pacifiques. Si Industriel A augmente sa puissance commerciale par exemple, Industriel B à deux options ; soit il interprète cette augmentation commerciale comme défensive et ne répond pas, alors son insécurité augmente, au sens de la définition d'Arnold Wolfers, car le différentiel de puissance s'accroît. Soit Industriel B interprète cette augmentation de la puissance de Industriel A comme offensive, et il augmente ses propres capacités en retour. Son insécurité augmente également, car cela va inciter Industriel A à faire de même et relancer un cycle d'accroissement de sa puissance : la réaction de Industriel B confirme ses craintes initiales, s'il en avait, ou en génère sur la disposition de Industriel B s'il n'en avait pas.

[167] ***Cahiers de la Guerre Économique, La nouvelle intelligence juridique #6***, édition Les influences, 2022

[168] **ANSSI. Tensions Internationales : Renforcement de la vigilance cyber. 2022**. [En ligne] 14 mars 2022 ; 26 février 2022. [Consulté en mai 2022.] https://www.ssi.gouv.fr/actualite/tensions-internationales-renforcement-de-la-vigilance-cyber/

[169] **Portail de l'IE.** Dissuasion (par l'information). [En ligne] inconnue. [Consulté en mai 2022.] https://portail-ie.fr/resource/glossary/73/dissuasion-par-linformation

[170] **JSTOR.** Journal article Cooperation Under the Security Dilemma. [En ligne] [Consulté en mai 2022.] https://www.jstor.org/stable/2009958

Cette approche théorique tirée de la sécurité internationale retranscrit bien le climat durant la Guerre froide avec la course à l'armement et de nos jours, avec l'élargissement (soutenue par les États-Unis) de l'OTAN à l'Est de l'Europe perçue comme une menace par la Russie.

Pour des entreprises (ou des États), c'est un dilemme car il n'y a pas besoin de volonté délibérée de l'un ou de l'autre des acteurs pour s'enclencher. Renforcer ou développer sa « puissance » ne repose pas toujours sur une intention hostile.

Mais la survie ou la pérennité d'une entreprise passe nécessairement par le renseignement de son écosystème (concurrents, fournisseurs, etc.) pour adapter sa position défensive, offensive ou de statu quo.

3.3.2.3. Fusion/Acquisition

S'investir dans des opérations de fusions et d'acquisitions (parfois appelée « Fusac ») sensibles sans un minimum d'anticipation peut se révéler être un cuisant échec à court ou à moyen terme.

Ce type d'opération suit un processus normé décomposé en plusieurs étapes qui se calcule en mois. Suffisamment, tout du moins, pour éveiller des intérêts économiques malintentionnés. Annoncer aux marchés une décision de Fusac vous positionne dans l'œil du viseur de malveillants plus ou moins aguerris.

Les jours suivants l'annonce de rachat, des acteurs malveillants (Concurrent, Groupe APT, etc.) peuvent, pour vous toucher ultérieurement, préinstaller une charge numérique malveillante au sein du système d'information de l'entreprise que vous comptez racheter. Cette charge pourra sur déclenchement d'un programme ou d'une action à distance (command&control) compromettre la pérennité de votre entreprise.

Comme en témoigne Cyrille Badeau[171] , l'enjeu réside dans la collecte d'informations avant le rachat. Certaines informations spécifiques peuvent être partagées dans un cadre contraint (White Room) ou strictement encadré dans une « data room » précise Olivier de Maison Rouge « car il n'est pas rare de voir de tels pourparlers échouer, une fois ces informations [confidentielles] transmises »[172].

Ainsi, pour Cyrille Badeau, l'entreprise acquéreuse doit partager les marqueurs concernant ses adversaires passés et parfois même de TTP (Tactics Technics & Procédures – c.f. "Le référentiel MITRE ATT&CK") pour appréhender les attaques nouvelles portées par ces mêmes groupes, ainsi que les règles de détection associées. Communiquer ces renseignements à la société visée par le rachat pourrait, à cette dernière, lui permettre de les ajouter à sa politique de surveillance dans les jours/mois suivants afin de mieux se préparer à une éventuelle attaque au lendemain de l'annonce et pour donner un avantage à l'équipe SSI le jour de la réunification des réseaux.

Bien entendu, l'efficacité de cette action est liée au niveau de maturité et de capacité de sécurité informatique de la société rachetée.

[171] **BADEAU, Cyrille. Fusion/Acquisition : pourquoi les entreprises doivent adopter une stratégie commune de cyber-renseignement. 2018** [En ligne] 9 novembre 2018 ; Mis à jour le 2 mars 2021 https://www.silicon.fr/avis-expert/fusion-acquisition-pourquoi-les-entreprises-doivent-adopter-une-strategie-commune-de-cyber-renseignement

[172] ***Le droit du renseignement***, éditions LexisNexis, avril 2016

3.3.3. Éthique

3.3.3.1. L'éthique est-elle compatible avec le renseignement ?

Pour Michael Herman, « l'objectif du renseignement n'est pas de « faire du mal » à qui que ce soit. C'est une activité neutre destinée à fournir au décideur les éléments rationnels les plus justes et les plus objectifs possibles, afin que ce jugement soit raisonné et équilibré. »[173]

Selon Alain Juillet[174], l'éthique est une transcription de la morale dans une société en pleine évolution dans laquelle on ne peut pas échapper aux rapports de force.

3.3.3.2. La guerre économique juste

Selon Daniel Brunstetter et Jean-Vincent Holeindre : « La théorie de la guerre juste considère qu'il est impossible de séparer la morale et la guerre, et qu'il est donc nécessaire d'établir des liens entre les deux termes. Elle forme un « ensemble d'idées et de valeurs relatives à la justification morale d'une guerre. Elle propose une série de règles morales que les sociétés doivent appliquer au début, au cours et à la fin de la guerre (Biran Orend). » Des critères pertinents sont établis pour justifier l'intervention militaire et pour encadrer les actions militaires, voire pour assurer de manière juste la sortie de la guerre.

L'Intelligence Economique est une discipline jeune qui dispose d'un cadre déontologique. Une charte d'éthique[175] a été produite par le Syndicat Français de l'Intelligence Economique (SYNFIE).

Cette charte a pour objet de proposer et de conférer un cadre éthique aux activités professionnelles de ses membres. Chaque adhérent du SYNFIE s'oblige par voie de conséquence à respecter et à faire respecter à ses salariés et représentants les termes et engagements découlant de la présente Charte.

Ainsi, nous conseillons les dirigeants à se rapprocher des membres du SYNFIE pour éviter de faire intervenir des officines plus ou moins sérieuses qui, sous couvert de l'Intelligence Économique, pratiquent des activités illégales.

3.3.3.3. Le renseignement « entre amis »

Tel que le soulignent Olivier Chopin et Benjamin Oudet, « il est coutume de dire qu'il n'y a pas de services de renseignement amis mais des services de renseignement de pays amis ».

Dans l'entreprise, par essence, seule la performance et les intérêts comptent. En ce sens, l'Intelligence Économique permet d'apporter un cadre légal à cette mission naturelle que ce soit dans son application avec l'environnement concurrentiel ou de vos fournisseurs, actionnaires et partenaires.

La collaboration n'implique pas la confiance totale. En effet, il faut rester attentif. Les informations échangées ou transmises pourraient être utilisées à d'autres fins que pour lesquelles elles ont été partagées.

---

[173] *Renseignement et sécurité*, édition Armand Colin, 2019

[174] **FORSTER**, **Christophe.** COLLOQUE AAIE-IHEDN « INTELLIGENCE ECONOMIQUE ET ETHIQUE » [En ligne] date inconnue. [Consulté en mai 2022.] https://ie-ihedn.org/wp-content/uploads/2012/01/COLLOQUE-AAIE-IE-ETHIQUE.pdf

[175] **SYNFIE.** La charte d'éthique. [En ligne] inconnue. Charte adoptée le 15 avril 2014 [Consulté en mai 2022] https://synfie.fr/le-synfie/la-charte-dethique/

3.3.4. Le droit du renseignement en France

En complément de la partie « l'Environnement et cadre législatif », nous apportons à votre connaissance le droit lié au renseignement appliqué à deux catégories d'entreprise en France.

3.3.4.1. Appliqué aux entreprises concourant à la défense et à la promotion des intérêts fondamentaux de la Nation

Face à l'environnement stratégique actuel, le renseignement relatif à la défense et à la promotion des intérêts fondamentaux de la Nation est une pratique légale pour les entreprises ayant la nécessité de répondre aux enjeux de sécurité et de défense nationale.

Nous pensons ici tout particulièrement aux entreprises désignées d'importance vitale par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) et à leurs fournisseurs (dont les systèmes d'information auront été identifiés d'importance vitale par leurs clients). Ces derniers sont tenus, eux aussi, de se mettre en conformité avec la Loi de Programmation Militaire (LPM).

La Loi dite LPM dans son article 22 stipule :
« Art. L. 1332-6-1. – Le Premier ministre fixe les règles de sécurité nécessaires à la protection des systèmes d'information des opérateurs mentionnés aux articles L. 1332-1 et L. 1332-2 et des opérateurs publics ou privés qui participent à ces systèmes pour lesquels l'atteinte à la sécurité ou au fonctionnement risquerait de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation. Ces opérateurs sont tenus d'appliquer ces règles à leurs frais. »

Par ailleurs le décret d'application no 2015-351 du 27 mars 2015 relatif à la sécurité des systèmes d'information des opérateurs d'importance vitale précise :
« Art. R. 1332-41-2. – Chaque opérateur d'importance vitale établit et tient à jour la liste des systèmes d'information mentionnés à l'article L. 1332-6-1, y compris ceux des opérateurs tiers qui participent à ces systèmes, auxquels s'appliquent les règles de sécurité prévues au même article. »

Le même décret ajoute :
« Art. R. 1332-41-19. – Les opérateurs d'importance vitale prennent les mesures nécessaires, notamment par voie contractuelle, pour garantir l'application des dispositions prévues à la présente section aux systèmes d'information des opérateurs tiers mentionnés au premier alinéa de l'article R. 1332-41-2 »

3.3.4.2. Appliqué aux entreprises privées

Dans cette compétition économique mondiale et par la prolifération des nouvelles technologies et des informations en ligne, les entreprises privées peuvent désormais recourir à la pratique du renseignement économique à partir des sources ouvertes comme le précise C.Anno[176] : « contrairement à l'espionnage industriel, l'intelligence économique est légale.» Dans sa recherche d'information, elle met en œuvre des procédés légaux et respecte des codes d'éthique fixés par la Fédération des professionnels de l'intelligence économique, créée à la fin de l'année 2005 par l'amiral Pierre Lacoste. Depuis 2010 le Syndicat Français de l'Intelligence Économique (SYNFIE), nous donne une définition de l'intelligence économique : «

[176] **C. Anno. Le droit de l'Intelligence Économique. Le petit juriste. 2015.** [En ligne] 29 décembre 2015. [Consulté en mai 2022] https://www.lepetitjuriste.fr/droit-de-lintelligence-economique

L'intelligence économique se définit comme étant l'activité professionnelle qui vise à collecter, analyser, diffuser et protéger l'information économique stratégique ».

Nous l'avons développé précédemment (c.f. partie « Environnement et cadre législatif »), les entreprises privées peuvent pratiquer du renseignement économique avec des moyens de droit commun. Tout l'art réside dans l'usage « de méthodes éprouvées, nobles et vertueuses, éthiques et déontologiques, tout en parvenant à accéder à des informations non révélées, et néanmoins pertinentes » comme le souligne Olivier de Maison Rouge[177].

3.3.5. Pratiques complémentaires au cyber-renseignement

Nous l'avons vu précédemment, le renseignement utilisé dans les règles de l'art de l'Intelligence Économique est une pratique aujourd'hui applicable au profit des entreprises privées qu'elles se sentent ou non en situation de guerre économique (comme évoqué dans le chapitre "De la guerre à la guerre économique"). Le (cyber-)renseignement s'apparente donc à une collecte « active » valorisée par une démarche proactive. D'autres pratiques révélées ou non existent.

3.3.5.1. L'influence de terrain

En France, le domaine des relations interculturelles demeure très peu connu et de facto très peu appliqué tant dans la vie quotidienne que dans la vie économique.

Or, cela représente un réel manque dans une stratégie d'entreprise ayant des visées internationales. En effet, connaître les us et coutumes d'un pays dans lequel une entreprise cherche à s'implanter est plus que nécessaire. Une bonne connaissance des enjeux interculturels apporte plusieurs avantages :

- Éviter les impairs culturels malencontreux qui peuvent faire capoter la captation d'un marché ;
- Ouvrir l'esprit des collaborateurs aux réalités culturelles de « l'autre » pour éviter les jugements et autres comportements pouvant jouer sur les relations locales ;
- Être en mesure de prospecter, de créer un réseau en avance de phase pour être bien implanté localement et avoir une avance lors de la publication d'appels d'offres ;
- Faire de l'influence.

3.3.5.2. L'opération d'influence psychologique

Cette pratique est issue du domaine militaire. Tout reste à croire qu'elle est aujourd'hui employée, de manière confidentielle, dans le domaine économique.

Olivier Chopin et Benjamin Oudet l'affirment, « L'information warfare[178] (IW) est l'un des sujets majeurs des discussions stratégiques contemporaines et s'est imposée comme un aspect fondamental des conflits au XXIe siècle. Il n'existe aucune définition consensuelle de l'IW et aucun concept n'est encore cristallisé. Cependant, nombreux sont ceux à admettre son importance dans les conflits contemporains et il est d'emblée nécessaire d'en analyser les objectifs. Tout l'enjeu est de peser sur le processus de décision de l'ennemi, que ce soit dans les domaines militaire, politique, économique ou une combinaison des trois…

[177] *Le droit du renseignement*, éditions LexisNexis, avril 2016
[178] Guerre de l'information

Ces opérations (ndlr psychologiques) sont menées pour diffuser à une cible donnée des informations sélectionnées afin d'influencer ses émotions, ses motivations, ses objectifs et *in fine* son comportement et ses décisions. »

Les entreprises ont à leur disposition bon nombre de moyens pour mener des opérations psychologiques. Le font-elles ? Oui, vraisemblablement.

3.3.6. Techniques de renseignements offensifs

Dans son livre[179], Philippe Dylewski en dénombre 300. Il faut faire preuve toutefois de vigilance. Certaines pratiques comme l'espionnage, la manipulation, la corruption, etc. ne rentrent pas dans le registre de « l'intelligence économique et stratégique » car les renseignements sont obtenus de manière illégale.

Nous citons ici l'ouvrage de Philippe Dylewski car l'objectif affiché de l'auteur est aligné avec le cadre déontologique de l'Intelligence Économique :

« En aucun cas je ne conseille d'espionner un concurrent dans le but de le copier. Seulement pour faire mieux. Pour ne pas être largué. Surveiller vos concurrents, c'est apprendre de leurs forces et de leurs faiblesses, ce qui fonctionne et ce qui ne fonctionne pas. Il s'agit d'apprendre et de grandir ».

Loin de nous l'idée de dresser ici la liste pléthorique de techniques et d'outils d'investigation employées dans le domaine cyber et en dehors. Nous avons pour objectif de sensibiliser à quelques-unes d'entre elles pour démontrer la facilité d'accès aux informations.

1. **Moteurs de recherche**

Le monopole de Google, fait de lui une base de renseignement inévitable. Toutefois, si les recherches adressent la Russie ou la Chine, il convient d'utiliser des moteurs locaux à savoir respectivement Yandex et Baidu (se référer au chapitre « La e-réputation » pour plus d'informations).

Il est possible d'effectuer des recherches de bases (qui se limiteront à une profondeur réduite visible d'Internet) ou avancées pour trouver des vidéos, des images, du texte, des informations (issues de journaux, blogs, tweets, réseaux sociaux…) à l'aide :

- D'opérateurs booléens : « » (suite de termes dans un ordre précis); OR (retourne les résultats de l'un ou l'autre des termes) ; + (associer des termes) ; ~ (réduit ou élargi les recherches) ; - (exclure des termes) ; € ou $ (obtenir le prix d'un produit ou service) ; .. (allant de.. à..) ; etc.
- D'opérateurs de recherches très utiles (dénommés dorks) :
- « intitle : » sur le titre d'une page,
- « site: » sur un site spécifique,
- « related: »permet de situer votre référencement et d'identifier vos concurrents, etc.

Ces opérateurs, permettant d'accéder à des sources ouvertes (informations accessibles publiquement), pourront être utilisés de manière unitaire ou conjuguée dans la même requête.

[179] **DYLEWSKI, Philippe.** ***Le Renseignement Offensif : 300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs*****,** édition Agakure, 2022. ISBN : 9791096819287

Google dispose également de fonctionnalités intégrées :

- De recherches avancées (accessibles depuis les paramètres).
- Pour prévenir en temps réel de toute modification de contenu susceptible d'intéresser la personne effectuant la recherche (sujets, concurrents…) ou de savoir ce qui est dit sur elle via Google Alert,
- de consulter des publicités sur des cibles (tiers, concurrents…), des reportages (bienveillant ou malveillant) sur un secteur d'activité spécifique ou une société par l'usage de Google Video, etc.

D'autres moteurs (ou métamoteurs) de recherches existent à l'instar de « Intelligence X » qui intègre de multiples outils ou moteurs (shodan, spyse, etc.) moins faciles d'accès.

Ces recherches associées à la discipline d'OSINT, permettent d'identifier ses vulnérabilités exposées sur Internet (informations rendues publiques, les mauvaises configurations réseaux, etc.) et renforcer la protection mais attention toutefois, cela peut engendrer des risques liées à la collecte de données relatifs aux tiers. En effet, Google a pour principe de tout traquer / tracer de nos activités pour eux-mêmes ou le compte de tiers.

Comme le stipule Philippe Dylewski, les entreprises peuvent être confrontées à trois risques liées à l'application de l'OSINT :

1. Le risque d'être détecté
2. Le risque de perdre l'accès à ces informations
3. Le risque de devenir la victime

A cette liste, nous devons également ajouter le risque légal lié la veille et l'investigation en ligne (c.f. partie "Environnement et cadre législatif"). Cependant, les entreprises pourront les utiliser sans craintes pour investiguer sur leurs propres systèmes dans la limite de ne pas collecter les données personnelles des salariés.

Collecter de l'information n'est pas une fin en soi.

La profusion d'information fiables et non fiables toujours plus importante, nécessitera de sourcer l'information c'est à dire de s'assurer de la crédibilité de ces informations. Ce qui est une tâche plus longue que celle de la collecte.

Des logiciels du marché pourront faire gagner du temps sur les collectes et l'analyse corrélée des informations. Nous citons ici une brève liste :

- Maltego : permet d'explorer les données et de produire sous la forme de graphique les relations entre ces données ;
- NexVision : initialement utilisé par l'armée et les gouvernements mais depuis 2020 ce logiciel est disponible à toute catégories d'entreprises pour leurs besoins en matière de renseignement et d'enquête ;
- Geocreepy : outil de renseignement de géolocalisation à partir de diverses plates-formes de réseaux sociaux et des services d'hébergement d'images.

Certains de ces logiciels disposent d'une version gratuite limitée toutefois en fonctionnalités.

Toutes ces technologies demandent à être utilisées au quotidien et de préférence par des compétences dédiées (internes ou externes) spécialisées (se référer au chapitre « Métiers et Disciplines Cyber » pour plus de détails).

2. La « collecte directe »

S'abonner à la newsletter ou se rendre à des évènements et salons professionnels sont autant de moyens simples d'obtenir de riches informations sur l'actualité de ses concurrents, leurs forces et faiblesses commerciales, leurs innovations, etc.

Et puis au-delà du cyber, pour ceux que cela ne dégoûte pas, il est possible de faire les poubelles de leurs sièges ou filiales. Elles peuvent être riche en matière d'informations !

3. Enquête de marché

L'analyse concurrentielle, par la sollicitation d'un cabinet spécialisé, permettra de recueillir des données bien utiles afin d'identifier les concurrents, d'adopter une nouvelle stratégie, etc.

4. Surveiller les brevets

Les dossiers de brevets sont publiés intégralement dix-huit mois après la date de dépôt. Le fait de suivre les brevets de ses concurrents et partenaires (où qu'ils soient déposés), permettra de se situer. Exemples:

- En France : https ://www.daata.gouv.fr/fr/organizations/institut-national-de-la-propriete-industrielle-inpi
- Au niveau Européen : https ://www.epo.org
- Au niveau mondial : https ://patents.google.com/

5. Suivre les modifications d'un site

Toute modification apportée sur un site Internet est tracée dans des outils en ligne (tel que trackengine.com). Il est possible de surveiller tout changement (de prix, de stock, etc.) sur les sites de ses concurrents et partenaires.

Le moteur « waybackmachine » sur le site archive.org. permet également visualiser l'évolution des changements des sites web de ses concurrents et partenaires.

6. Suivre la stratégie marketing numérique de vos concurrents

Pour ressortir en tête des recherches sur Internet, les entreprises doivent référencer des mots-clés pour améliorer leurs visibilités et trafics sur leurs sites web. En utilisant « SEMRush », il est possible consulter ce que font les concurrents et, entre autres, leurs stratégies marketing.

7. **Consulter les banques de données publiques nationales**

Les banques de données publiques regorgent de renseignements sur une situation passée des entreprises. Nous citerons ici, certaines d'entre elles, sur la marché Français :

- Infogreffe.fr et societe.com (fortement concurrencés par pappers.fr)
- Annuaire-entreprises.data.gouv.fr
- Bodacc.fr
- Data.inpi.fr

8. **Le renseignement humain (HUMINT)**

L'HUMINT vient parfois compléter les autres techniques ou c'est une voie de recours à sous-traiter quand les autres ne fonctionnent pas. L'usage des comportements d'influence est à maîtriser. A ce titre nous recommandons, pour s'assurer de rester dans la légalité, de faire appel à un cabinet spécialisé.

3.3.7. Métiers et disciplines « Cyber »

Les nouvelles opportunités de renseignements immenses offertes (par les sources d'information comme Internet ou les réseaux sociaux) entraînent de nouveaux métiers qui se situent entre le renseignement humain et technologique :

- L'HUMINT (human intelligence) destiné au renseignement d'origine humain (ROHUM). Il vise également la gestion et la sécurisation des sources de renseignements humains.
- Le SOCMINT (social media intelligence) destiné à collecter les informations générées par les réseaux sociaux.
- Le GEOINT (geospatial intelligence) destiné à collecter et à fusionner des données géolocalisées (à partir de tout capteur et toute source disponible) pour préciser des faits dans leurs environnements.
- L'IMINT (imagery intelligence) destiné à interpréter des images, des photos prises par satellite, avion, drone.
- Le SIGINT (signal intelligence) destiné au renseignement d'origine électromagnétique.

Ces métiers s'appuient également sur des disciplines de renseignements tel que :

- L'OSINT (sources ouvertes). C'est sans équivoque la plus connue intégrée généralement au départ d'un cycle de renseignement pour fournir des renseignements provenant d'une liste étendue de sources : Internet, réseaux sociaux, médias, etc.
- Le PROTINT (protected intelligence) discipline proche de l'OSINT, destiné à collecter des informations générées par toute action électronique susceptible de laisser des traces digitales.
- Le MASINT (measurement and signature intelligence) mesure des radiations utile notamment dans le domaine industriel.
- L'ELINT (electronic intelligence) utilisée pour capter et intercepter des ondes.
- Le COMINT (communications intelligence) utilisé pour capter les communications.

Au-delà de ces métiers, la fonction de RSSI dans certaines structures doit évoluer en Responsable de la Veille et du Renseignement (ou Responsable de l'Intelligence Économique) car, nous l'avons vu précédemment l'activité de Sécurité (ou de protection du patrimoine informationnel) du Système d'Information, que porte le RSSI, fait partie intégrante des missions de l'Intelligence Économique.

Sans équipe structurée à disposition, l'entreprise devra s'appuyer auprès de sociétés spécialisées en Intelligence Économique.

3.3.8. Constitution de la cellule d'Intelligence Economique

Plusieurs profils sont nécessaires pour adresser les activités d'une cellule d'Intelligence Économique. Voici les principaux :

Le Data Architect : élabore la structure des systèmes de gestion de données. Le rôle du Data Architect ou Architecte Big Data est d'agréger les données internes et externes pour ensuite concevoir un moyen de les regrouper et de les organiser. Il développe ensuite des modèles de données pour les structures de bases de données et va ensuite dessiner, documenter, construire et déployer des architectures et des applications de base de données. Les fonctionnalités techniques comme la scalabilité, la sécurité, la performance, la data recovery sont des préoccupations constantes de sa mission.

L'analyste / le veilleur : chargé de recueillir, analyser et synthétiser les éléments nécessaires à la présentation de la situation opérationnelle en temps réel.

Le Responsable IE : participe aux revues de projets avec l'équipe des chargés de missions, experts en innovation. Il se tient en permanence à jour de tout ce qui se fait en externe en matière d'intelligence économique.

Par ailleurs, le marché est en recherche constante de profils techniques, rompus aux mécanismes d'attaque et de protection, capables de répondre aux enjeux de cybersécurité. La filière cyber française est pourtant ambitieuse, puisqu'elle souhaite passer de 37.000 emplois en 2021 à 75.000 en 2025. [180] Pourtant, une telle augmentation constitue un réel défi puisque les formations spécialisées souffrent d'un manque de candidats et de professeurs. Cette situation n'est pas nouvelle puisque selon les propos de Charles Preux, directeur de la formation cyberdéfense de l'Ecole Nationale Supérieure d'Ingénieurs de Bretagne Sud (ENSIBS), en 2015, seuls 25 à 30 étudiants uniquement étaient diplômés chaque année[181].

> *« On a arrêté d'ouvrir des formations en masse car il n'y avait pas d'élèves, pas de profs. On s'est rendu compte qu'il fallait aussi que nous arrêtions de ne former que des élèves étrangers »* Guillaume Poupard, Directeur de l'ANSSI.

Pourtant, une étude réalisée par Michael Page en 2021 montre que bien que 80% des entreprises rencontrent des difficultés à recruter des experts de l'IT alors que 36% des candidats en recherche d'emploi n'ont aucune piste. Cela vient notamment du manque de profils aux compétences adaptées aux problématiques des entreprises[182].

[180] **DUBOIS, Marion. 2021.** Cybersécurité : la filière recrute mais peine à former ses élèves. *Ouest France*. [En ligne] 22 septembre 2021. [Consulté le 28 févier 2022.] https://www.ouest-france.fr/economie/cybersecurite-la-filiere-recrute-mais-peine-a-former-ses-eleves-13ac45e4-118a-11ec-aae0-4d1212b14fe9.

[181] **GUIRNARCHAUD, Angèle. 2015.** Entreprise recherche (jeunes diplômés) hackers désespérément. *Le Monde*. [En ligne] 13 juin 2015. [Consulté le 28 février 2022.] https://www.lemonde.fr/etudes-superieures/article/2015/06/13/entreprise-recherche-jeunes-diplomes-hackers-desesperement_4653663_4468191.html.

[182] **KALUSEVIC, Sacha et GOBRON, Gilles. 2021.** *Panorama du marché de l'emploi et du recrutement SI. Paris.* : Michael Page & Choose Your Boss, 2021.

Au niveau de l'expérience des professionnels de l'IT, une grande majorité (80%) font état de plus de 8 ans d'expérience. L'un des réels leviers afin de pourvoir les postes vacants en termes de cybersécurité : la formation. En effet, 54% des professionnels suivent ou ont suivi des formations ayant pour but de développer de nouvelles compétences. Au lieu de rechercher la perle rare opérationnelle immédiatement et cochant toutes les cases, il peut être intéressant de s'appuyer sur des profils polyvalents (39% des professionnels de l'IT occupent de postes transverses) qui peuvent bénéficier de formation plus techniques et spécifiques (la part des experts cyber ne représente que 3% des professionnels).

Le sujet est identique concernant les profils de data-scientists, qui seront capables d'avoir une vision d'ensemble des données, d'identifier celles qui sont vraiment stratégiques et de les mettre en valeur pour les présenter et décrire à leur direction [183] . Une direction qui, elle aussi, se devra d'être formée et sensibilisée à ces sujets afin de prendre les bonnes décisions.

L'idéal serait un profil hybride entre connaissances techniques de défense et d'attaque, d'organisations et de surveillance / mise en valeur de la donnée.

3.3.9. Conseils clés pour bâtir sa cellule d'intelligence économique

1. Détenir l'accord et l'implication du dirigeant dans ce projet.
2. Partant de zéro, faites appel à une société de conseil spécialisé en intelligence économique (de préférence, un membre du SYNFIE comme gage de professionnalisme).
3. Rédiger un code d'éthique interne et ne négligez pas la politique de sécurité.
4. Déterminer ce que vous souhaitez et devez savoir que ce soit en interne et en externe.
5. Procéder à un audit de renseignement pour produire une cartographie de vos sources d'informations et de renseignements.
6. Avec l'aide d'un Data Architect, concevez le socle technique qui permettra d'agréger les données internes et externes nécessaire à l'analyste.
7. Préparer les objections et la communication interne.
8. Impliquer le Comex, les directions et motiver vos salariés.

[183] **TROUCHAUD, Philippe. 2016.** *La Cybersécurité au-delà de la technologie.* Paris : Odile Jacob, 2016. p. 47. ISBN : 978-2-7381-3368-7.

Chapitre 4

Enquête sur les outils d'évaluations et d'autoévaluation de sa ressource informationnelle disponible en source ouverte

L'objectif de cette partie est la proposition d'un modèle d'autodiagnostic d'évaluation de la ressource informationnelle par les dirigeants d'entreprises.

En conséquence, il a été initié la démarche suivante :

1. Recensement des référentiels d'évaluation en intelligence économique disponibles en source ouverte.
2. Détermination des critères d'appréciation de ces outils d'évaluation.
3. Présentation et synthèse de la grille d'appréciation des référentiels.
4. Proposition des critères retenus pour le modèle d'autodiagnostic (en partie 3).
5. Présentation du modèle d'autodiagnostic (détaillé en 300 question et opérationnel en 25 questions).
6. Présentation d'un modèle graphique du niveau de maturité

4.1. Recensement des référentiels d'évaluation en intelligence économique disponibles en source ouverte

Dans une démarche de recherche d'informations relatives à des grilles d'évaluation de la ressource informationnelle, il a été choisi d'effectuer un recensement des outils francophones présents en intelligence économique disponibles en source ouverte.

Sur ce postulat de départ, il est ressorti que les guides pratiques et/ou les grilles d'analyses provenaient de façon récurrente de sources communes. En effet, sur la base des recherches sur le web, de nombreux ouvrages sont édités par les différentes chambres de commerce et d'industrie (C.C.I) en s'appuyant sur les ressources du Service de l'Information Stratégique et de la Sécurité Économique (SISSE).

Pour rappel, le S.I.S.S.E., rattaché à Bercy est chargé d'animer, sous l'autorité du Commissaire à l'information stratégique et à la sécurité économique (également Directeur général des entreprises), la politique de sécurité économique française. Le S.I.S.S.E. provient de la transformation en janvier 2016 de la Délégation Interministérielle à l'Intelligence Économique (D2IE) et du Service de coordination à l'intelligence économique (S.C.I.E.).

En conséquence, il sera présenté dans un souci d'exhaustivité des documents de sources différentes :

- Un ouvrage « généraliste grand public » : « *Le guide de l'intelligence économique. Le Routard* » rédigé en 2014 en collaboration avec la D2IE[184].

- Le guide de référence « *La sécurité économique au quotidien en 28 fiches pratiques* » rédigé en 2021 par le S.I.S.S.E.[185]

- L'ouvrage « *Intelligence économique. Un guide pour débutants et praticiens* » élaboré en 2002 dans le cadre du programme européen CETISME (Co-operation to promote economic and technological influence in small and medium-sized enterprises) partenariat formé d'iDeTra S.A.,

[184] **GLOAGUEN, Philippe.** Le guide l'intelligence économique. Le Routard. [en ligne]. 1° édition. Italie : HACHETTE LIVRE 2014. 143 pages. ISBN-301-00-00-03-62-96 [consulté le 12 mai 2022]. Disponible à l'adresse : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/routard-guide-intelligence-economique.pdf

[185] **Service de l'Information Stratégique et de la Sécurité Économique (S.I.S.S.E.).** La sécurité économique au quotidien [en ligne]. Novembre 2021. 95 pages. ISBN-978-2-11-152646-4. [consulté le 12 mai 2022]. Disponible à l'adresse : https://sisse.entreprises.gouv.fr/files_sisse/files/outils/fiches/la-securite-economique-au-quotidien-en-28-fiches.pdf

Dirección Regional de Investigación - Comunidad de Madrid, du Conseil Régional de Lorraine, de Coventry University Enterprises Ltd et de Consorzio Pisa Ricerche, ATTELOR et Meta Group. Intelligence économique[186].

- Le guide «*Intelligence économique. Guide à L'attention des PME de Suisse Romande.* » élaboré en 2017 par la Haute Ecole de Gestion de Genève[187].
- La thèse « *Modèle d'évaluation de la réussite d'un système d'intelligence économique (M.E.R.S.I.E)* » rédigée en 2008 dans le cadre d'un doctorat de l'Université de Lorraine[188].
- Le logiciel de diagnostic d'intelligence économique (DIESE)[189].

4.2. Détermination des critères d'appréciation de ces outils d'évaluation

4.2.1. Définition des critères d'appréciation

Afin de pouvoir comparer ces différents ouvrages, il a été défini cinq critères de comparaison :

- L'exhaustivité des domaines visés par les questionnaires et/ou fiches pratiques proposés.
- La praticité des outils pour la mise en œuvre d'une démarche efficace d'intelligence économique.
- La hiérarchisation des mesures proposées afin de cibler les actions les plus efficaces à mettre en place au début de la démarche.
- L'évaluation de la maturité de l'entreprise par rapport à l'intelligence économique et/ou la ressource informationnelle.
- L'évaluation du coût des mesures (pour s'attacher aux mesures coût modéré/impact fort).

Le critère sera apprécié à l'aide d'une grille à quatre niveaux présentée en pages suivantes.

---

[186] **CETISME (Co-operation to promote economic and technological influence in small and medium-sized entreprises)** partenariat formé d'iDeTra S.A., Dirección Regional de Investigación - Comunidad de Madrid, du Conseil Régional de Lorraine, de Coventry University Enterprises Ltd et de Consorzio Pisa Ricerche, ATTELOR et Meta Group. Intelligence économique. Un guide pour débutants et praticiens. [en ligne]. 2002. 97 pages. ISBN-84-451-2389-0. Disponible à l'adresse : https://www.madrimasd.org/sites/default/files/intelligence-economique-guide-integral.pdf

[187] **MADINIER, Hélène. Haute école de gestion Genève. Intelligence économique. Guide à l'attention des PME de Suisse Romande**. [en ligne]. 2ème édition, février 2016 (liens mis à jour en janvier 2017). 35 pages. [consulté le 12 mai 2022]. Disponible à l'adresse : http://www.jveille.ch/wp-content/uploads/2019/02/guide_ie_pme_version_16_17.pdf

[188] **DHAOUI, Chedia. Université de Lorraine. Les critères de réussite d'un système d'intelligence économique pour un meilleur pilotage stratégique : Proposition d'un Modèle d'évaluation de la Réussite d'un Système d'Intelligence Économique** [en ligne]. Thèse présentée et soutenue le 04 avril 2008. 610 pages. p 547-571. [consulté le 12 mai 2022]. Disponible à l'adresse : https://hal.univ-lorraine.fr/tel-01752721/document

[189] **Délégation interministérielle à l'intelligence économique (appelée Service de l'Information Stratégique et de la Sécurité Économique (S.I.S.S.E.)** 12 mai 2012. - Diagnostic d'intelligence économique et de sécurité des entreprises (D.I.E.S.E.) [en ligne]. Avril 2014. [consulté le 12 mai 2022]. Disponible à l'adresse : https://sisse.entreprises.gouv.fr/fr/ressources/diese

4.2.2. Définition des niveaux d'appréciation

Critère d'appréciation	Niveau	Définition du niveau
EXHAUSTIVITÉ	1	L'outil n'est absolument pas exhaustif
	2	L'outil n'aborde que quelques domaines de l'intelligence économique
	3	L'outil identifie les domaines principaux de l'intelligence économique
	4	L'outil couvre l'intégralité du spectre de l'intelligence économique

Critère d'appréciation	Niveau	Définition du niveau
PRATICITE	1	L'outil ne permet pas de mettre en œuvre une démarche d'intelligence économique
	2	L'outil permet d'initier une réflexion d'intelligence économique
	3	L'outil permet de construire une démarche d'intelligence économique
	4	L'outil est directement utilisable par les entreprises

Critère d'appréciation	Niveau	Définition du niveau
HIÉRARCHISATION	1	Il n'existe aucune hiérarchisation des mesures
	2	La hiérarchisation des mesures est évoquée
	3	Une hiérarchie simple des mesures est proposée
	4	Une hiérarchisation des mesures est définie et structurée

Critère d'appréciation	Niveau	Définition du niveau
MATURITÉ	1	Le degré de maturité de l'entreprise à l'intelligence économique n'est absolument pas abordé
	2	Le degré de maturité de l'entreprise à l'intelligence économique est abordé
	3	Une première évaluation de la maturité de l'entreprise à l'intelligence économique est proposée
	4	Un modèle d'évaluation de la maturité de l'intelligence économique est proposé

Critère d'appréciation	Niveau	Définition du niveau
COÛT	1	L'outil n'aborde pas le coût des mesures
	2	Les coût des mesures est évoqué
	3	Les mesures sont évaluées financièrement
	4	Le coût des mesures est évalué et hiérarchisé

4.2.3. Présentation et synthèse de la grille d'appréciation des référentiels

4.2.3.1. Listing des différents référentiels revus

Référentiel d'intelligence économique	Critères d'appréciation					Synthèse	
	Exhaustivité	Praticité	Hiérarchisation	Maturité	Coût	Forces	Faiblesses
LE GUIDE DE L'INTELLIGENCE ÉCONOMIQUE – LE ROUTARD – 2014[1]	2	2	2	2	1	▪ Un panorama de l'intelligence économique ▪ De nombreux contacts utiles, sites référencés, moteurs de recherche… ▪ Des témoignages de différents acteurs du monde économique	▪ Pas de structuration concernant une mise en œuvre pratique d'une politique d'intelligence économique (hiérarchisation des mesures peu abordée..) ▪ Un document trop généraliste et superficiel
LA SÉCURITÉ ÉCONOMIQUE AU QUOTIDIEN en 28 fiches pratiques SISSE – Novembre 2021[2]	4	3	2	2	1	▪ Un guide récent de 28 fiches pratiques très exhaustif ▪ Un ensemble de mesures structurées sur une répartition Comportemental /Organisationnel / technique ▪ Des mots clés et contacts utiles pour chaque fiche pratique	▪ La hiérarchisation des mesures et la maturité du système sont peu abordés ▪ Aucune référence au coût des mesures
INTELLIGENCE ECONOMIQUE. UN GUIDE POUR DÉBUTANTS ET PRATICIENS – Projet européen CETISME – 2002[3]	4	2	3	3	1	▪ Un guide exhaustif scindé en 2 parties selon la maturité des entreprises ▪ Un comparatif des différentes pratiques européennes ▪ Des propositions de modèles et grilles d'analyses en l'intelligence économique	▪ Un document très complet mais trop académique ▪ Absence de fiches pratiques de mesures simples à mettre en oeuvre
INTELLIGENCE ECONOMIQUE. GUIDE À L'ATTENTION DES PME DE SUISSE ROMANDE – Haute école de gestion Genève – janvier 2017[4]	2	3	2	2	1	▪ Une méthodologie claire de mise en place d'une stratégie d'intelligence économique ▪ Un processus pas à pas d'analyse et de traitement de l'information	▪ Un manque d'outils pratiques (questionnaires….) pour documenter la démarche ▪ Une évaluation superficielle des outils en open source à disposition
MODELE D'EVALUATION DE LA RÉUSSITE D'UN SYSTÈME D'INTELLIGENCE ÉCONOMIQUE (MERSIE) – Thèse Université Lorraine – 2008 (Annexes 3 et 4)[5]	3	2	2	3	1	▪ Une volonté de créer un système d'évaluation mesurée de l'intelligence économique ▪ Une proposition de questionnaire s'attachant sur les facteurs internes de l'entreprise (culturels…) ▪ Une documentation théorique bibliographique importante	▪ Une démarche théorique due au type d'exercice (thèse) ▪ Une absence de modèle pratique synthétique de mise en œuvre
LOGICIEL DE DIAGNOSTIC D'INTELLIGENCE ÉCONOMIQUE ET DE SÉCURITÉ DES ENTREPRISES (DIESE) – Délégation interministérielle à l'intelligence économique – avril 2014	2	4	2	2	1	▪ Logiciel disponible gratuitement pour évaluer les vulnérabilités de son entreprise et son niveau de sécurité ▪ Un outil simple et facile d'utilisation	▪ Le questionnaire proposé aurait pu être plus fourni pour être plus opérationnel ▪ La ressource informationnelle est insuffisamment traitée

4.2.3.2. Synthèse générale de la grille d'appréciation

A la lecture de cette grille d'appréciation des référentiels économique, il est possible de retenir quelques tendances :

- Un tiers des référentiels peut être estimé réellement exhaustif.
- Un outil proposé est directement utilisable par les entreprises (cf le logiciel DIESE). Mais il faut noter la volonté du S.I.S.S.E. dans son dernier ouvrage de délivrer des fiches pratiques synthétiques, et organisées.
- La hiérarchisation des mesures est peu abordée par les différents référentiels.
- Les référentiels proposés traitent rarement de la maturité de l'entreprise relative à la ressource informationnelle. En l'occurrence, les deux documents s'y rattachant sont des ouvrages élaborés dans le cadre de recherches académiques.
- Aucune grille d'appréciation n'a une approche relative à la structuration du coût des mesures.

En conséquence, il est proposé la création de deux types d'autodiagnostic relatifs à la ressource informationnelle à destination des dirigeants d'entreprises :

- Un modèle théorique d'autodiagnostic destiné à des entreprises structurées en termes de préservation de leur ressource informationnelle
- Un modèle simplifié d'autodiagnostic destiné à des entreprises souhaitant avoir un retour rapide sur leur appétence à la préservation de leur ressource informationnelle

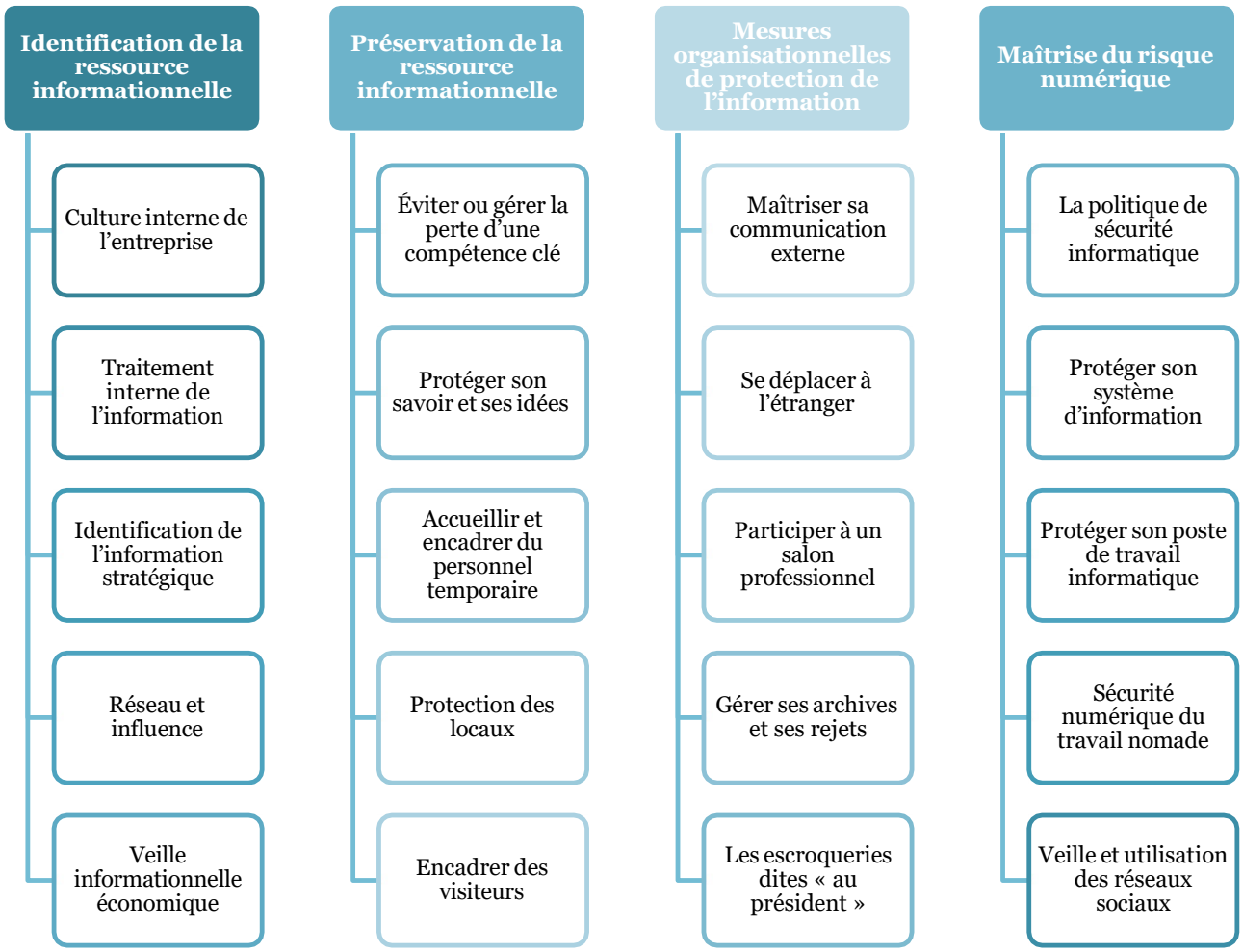
Chapitre 5

Proposition d'un modèle d'évaluation de la ressource informationnelle

L'autodiagnostic est structuré sur la base de quatre domaines (cadrans) :

- Identification de la ressource informationnelle stratégique
- Préservation de de la ressource informationnelle
- Mesures organisationnelles de protection de la ressource informationnelle
- Maîtrise du risque numérique

Ont été retenus cinq items par domaine et quinze questions par item sur une base de réponse (O/N).



5.2. Autodiagnostic théorique d'analyse de ressource informationnelle à destination des dirigeants d'entreprise

Nous proposons donc un autodiagnostic théorique complet comportant 300 questions (15 questions pour 5 thèmes pour 4 cadrans). **Cependant, conscients de la réalité opérationnelle des dirigeants d'ETI, nous proposerons un modèle simplifié de 25 questions.**

5.2.1. Proposition d'un modèle théorique d'évaluation de la maturité des entreprises à la ressource informationnelle (300 questions)

5.2.1.1. Définition des critères d'appréciation de la maturité par domaine

Chaque domaine sera apprécié à l'aide d'une grille d'évaluation à trois niveaux sur la base suivante :

DOMAINE	NIVEAU	DEFINITION DU NIVEAU DE MATURITE
Identification de la ressource informationnelle	0 < x ≤ 5	Votre entreprise n'a pas identifié sa ressource informationnelle.
	5 < x ≤ 10	Votre entreprise est en phase d'identification de sa ressource informationnelle.
	10 < x ≤ 15	Votre entreprise est engagée dans une logique d'identification de sa ressource informationnelle.
Préservation de la ressource informationnelle	0 < x ≤ 5	Votre entreprise est exposée à la prédation de sa ressource informationnelle.
	5 < x ≤ 10	La protection de votre ressource informationnelle peut-être accrue par de nouvelles actions.
	10 < x ≤ 15	Votre entreprise est consciente de l'importance de la préservation de sa ressource informationnelle.
Mesures organisationnelles de protection de l'information	0 < x ≤ 5	Les mesures organisationnelles de protection de l'information sont insuffisantes dans votre entreprise.
	5 < x ≤ 10	Votre entreprise doit engager de nouvelles mesures pour accroitre son niveau de protection de l'information.
	10 < x ≤ 15	Votre entreprise est structurée afin de protéger son information.
La maîtrise du risque numérique	0 < x ≤ 5	Votre entreprise est exposée à une attaque numérique.
	5 < x ≤ 10	Votre entreprise est sensibilisée au risque numérique.
	10 < x ≤ 15	Votre entreprise en engagée dans une politique de sécurité numérique.

5.2.1.2. Questionnaire détaillé

En raison du nombre important de questions, le questionnaire détaillé se trouve dans la partie Annexes de ce document.

La création d'un tel questionnaire, avec une granularité très fine, permettra à tout dirigeant qui le souhaite (accompagné des experts ou parties prenantes qu'il jugera utile) d'évaluer son niveau de maturité par rapport à l'état de l'art. Par ailleurs, les résultats étant aussi consultables par cadran, les dirigeants pourront focaliser leurs efforts sur un domaine en particulier selon le niveau de priorité stratégique qu'ils auront eux-mêmes fixé.

Nous recommandons donc vivement l'utilisation du questionnaire complet qui permet de balayer un spectre large et diversifié afin de limiter au maximum les angles mort.

Cependant, nous avons aussi travaillé sur une version plus opérationnelle reprenant les principaux thèmes qu'il ne faut pas négliger dans un contexte de guerre économique.

5.2.2. Proposition d'un modèle opérationnel simplifié d'évaluation de la maturité des entreprises à la ressource informationnelle à destination des dirigeants d'ETI

5.2.2.1. Définition des critères d'appréciation de la maturité globale pour modèle opérationnel

Contrairement au questionnaire détaillé, le questionnaire opérationnel ne sera pas évaluable par cadran, mais permettra au dirigeant d'avoir une note globale sur sa maturité. Ainsi, les principaux thèmes critiques seront repris et une grille d'analyse en 5 niveaux est proposée. Le principe est toujours le même à savoir des questions par lesquels les participants doivent répondre par Oui ou Non (1 point pour chaque réponse Oui), le total cumulé permettant d'avoir une note sur le niveau de maturité :

NIVEAU	SCORE	DEFINITION DU NIVEAU DE MATURITE
1	$0 < x \leq 5$	Votre entreprise est exposée à la prédation de sa ressource informationnelle
2	$5 < x \leq 10$	Votre entreprise n'est pas organisée pour identifier et préserver sa ressource informationnelle
3	$10 < x \leq 15$	Votre entreprise est sensibilisée à l'identification et la préservation de sa ressource informationnelle
4	$15 < x \leq 20$	Votre entreprise est engagée dans une politique d'identification et de préservation de sa ressource informationnelle
5	$20 < x \leq 25$	Votre entreprise a intégré sa politique d'identification et de préservation de sa ressource informationnelle dans une politique globale d'intelligence économique

5.2.2.2. Questionnaire opérationnel

Le modèle proposé s'attachera en 25 questions à décrire le panorama de l'identification et la préservation de la ressource informationnelle. L'objectif visé est la présentation d'un outil pratique permettant aux dirigeants d'entreprise d'avoir un retour rapide sur leur appétence à l'intelligence économique.

#	QUESTIONS	NON (0)	OUI (1)
1	Est-ce que l'information dans l'entreprise est perçue comme un facteur d'action ?		
2	Existe-t-il un échange de connaissances et un partage d'expériences au sein de l'entreprise ?		
3	Existe-t-il une procédure d'évaluation de la qualité des informations collectées ?		
4	Les destinataires des informations pertinentes sont-ils identifiés ?		
5	Procédez-vous à une capitalisation des connaissances stratégiques dans votre entreprise ?		
6	La structure organisationnelle de l'entreprise permet-elle le travail en mode réseau ?		
7	Menez-vous des actions d'influence pour préserver et renforcer les intérêts de votre entreprise (organismes de normalisation, décideurs publics locaux, ministères, ONG) ?		
8	Avez-vous une structure interne de de veille économique		
9	Avez-vous des sources d'informations internes et savez-vous les valoriser (savoir-faire du personnel , rapports de SAV..) ?		
10	Avez-vous cartographié les compétences clés en anticipant la stratégie de développement de l'entreprise et les perspectives du marché ?		
11	Identifiez-vous, parmi les différents titres de propriété intellectuelle (brevets, marques, dessins et modèles, droits d'auteur…) ceux qui sont les mieux adaptés pour valoriser vos innovations, vos produits et créations immatérielles ?		
12	Etablissez-vous une stratégie interne en matière de propriété intellectuelle ?		
13	Evaluez-vous périodiquement la performance du système de contrôle d'accès (audits internes, exercices, tests d'intrusion, délais d'intervention…) ?		
14	Elaborez-vous formellement une procédure d'accueil des visiteurs quels qu'ils soient ?		
15	Demandez-vous à tous les employés de l'entreprise de faire valider, préalablement et systématiquement, auprès de sa Direction, tout contact avec un journaliste, un analyste financier… ?		
16	Une procédure d'urgence de communication en cas d'incident est-elle mise en place dans l'entreprise ?		
17	Lors de déplacements à l'étranger, vous renseignez vous sur les législations locales en matière de chiffrement des données ?		
18	Mettez-vous en place une solution de suivi, un plan de classement et d'archivage spécifique pour les supports d'information dont le contenu est stratégique ?		
19	Sensibilisez-vous régulièrement tout le personnel (yc les stagiaires, les nouveaux arrivants…) aux escroqueries dites « au président » ou FOVI ?		
20	Votre entreprise s'est-elle dotée d'une politique de sécurité informatique ?		
21	Attribuez-vous des droits d'accès au réseau informatique (répertoires, calendriers..) de façon graduée et adaptée aux besoins ?		
22	Cloisonnez-vous les fonctions d'administration du reste du système d'information ?		
23	Veillez-vous à ce que vos salariés n'utilisent leurs appareils nomades personnels uniquement à des fins professionnelles ?		
24	Existe-t-il un processus de validation des communications sur les réseaux sociaux avant diffusion ?		
25	Mettez-vous en place une veille rigoureuse sur internet sur les noms de la société, de ses dirigeants et de ses marques afin de pouvoir réagir contre les dénigrements, les « cybersquats » out toute autre action préjudiciable ?		
RESULTAT			
SCORING = 0 < **x** < 25			

5.3. La représentation graphique du niveau de maturité de l'entreprise

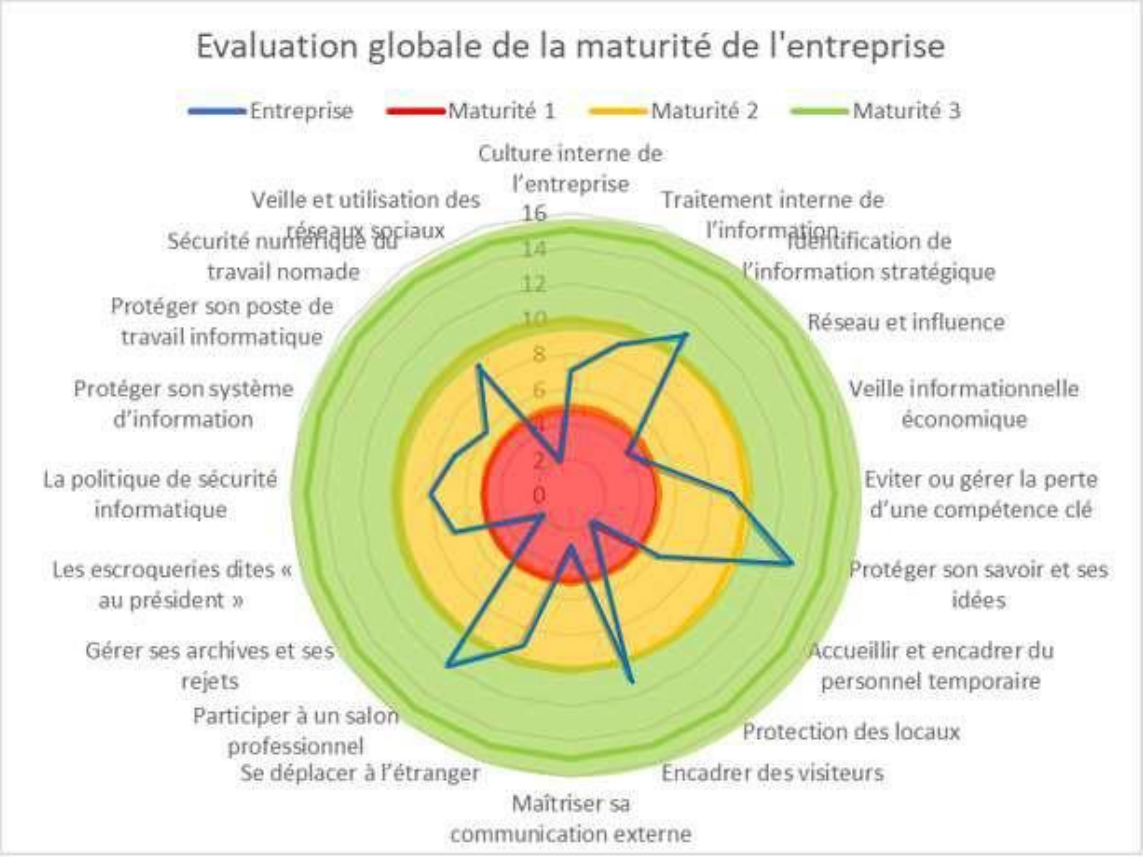
Il est proposé de présenter les niveaux de maturité de l'entreprise :

- A l'aide de la représentation globale des domaines d'étude
- A l'aide d'une représentation simplifiée pour chaque type de domaine

Des graphiques de type « toiles d'araignée » sont utilisés pour représenter les résultats de l'autodiagnostic à destination des dirigeants d'entreprises.

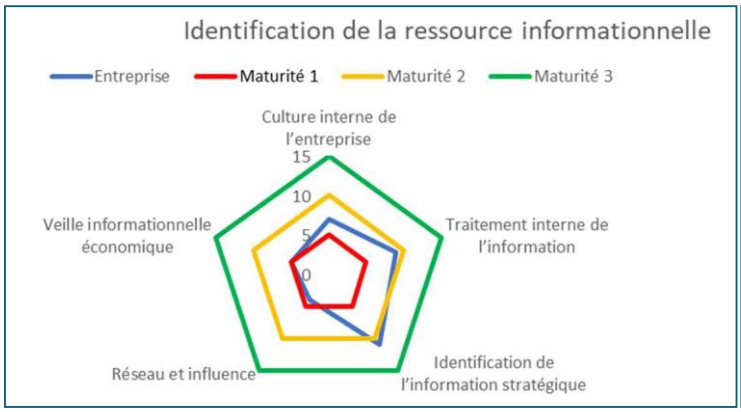
5.3.1. La représentation graphique globale de la maturité de l'entreprise

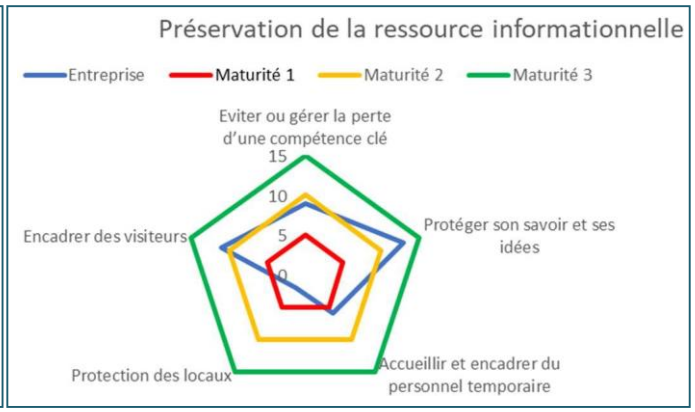
NIVEAU DE MATURITE	SCORE	DEFINITION
Maturité 1	0 < x ≤ 5	Votre entreprise n'est pas organisée pour identifier et préserver sa ressource informationnelle
Maturité 2	5 < x ≤ 10	Votre entreprise est sensibilisée à l'identification et la préservation de sa ressource informationnelle
Maturité 3	10 < x ≤ 15	Votre entreprise est engagée dans une politique d'identification et de préservation de sa ressource informationnelle

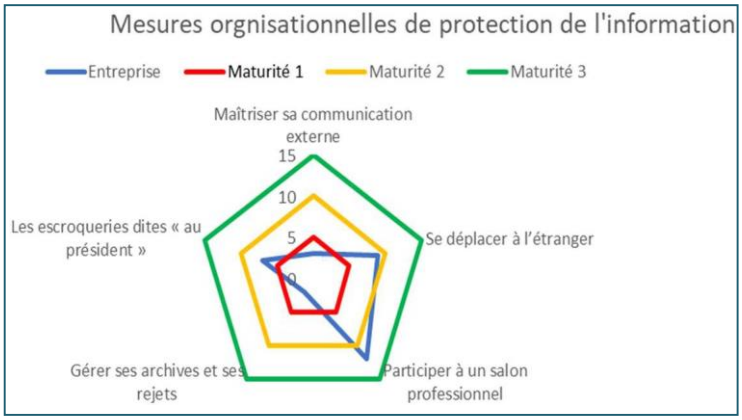


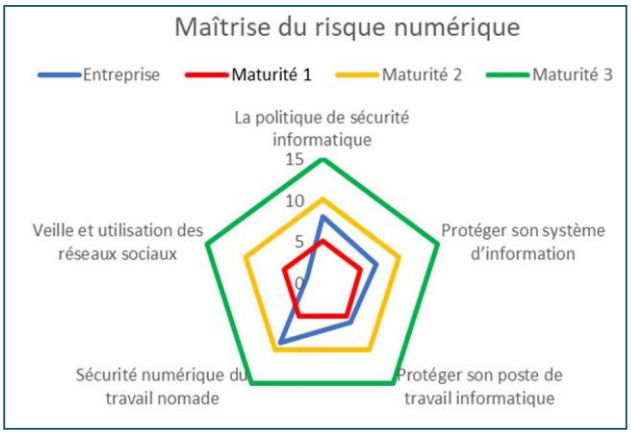
5.3.2. La représentation graphique pour chaque domaine de l'entreprise

Les niveaux de maturité de l'entreprise sont définis selon les critères mentionnés au chapitre **« critères d'appréciation de la maturité par domaine »**. Ci-dessous quelques exemples de résultats de questionnaires matérialisés par des graphiques.









Conclusion générale

Avec l'avènement de la société de l'information, l'information est désormais disponible pour tous les acteurs économiques. Dès lors, le véritable enjeu, pour les dirigeants soucieux d'assurer la pérennité de leur entreprise, est de maîtriser le paradoxe entre le besoin d'informations stratégiques pertinentes et la surabondance d'informations diverses et variées.

Les aspects négatifs de la société moderne de l'information, désinformation, espionnage industriel, tentatives de déstabilisation, cyber-intrusions, ou prédation d'informations stratégiques, amplifient ce paradoxe difficile à traiter pour tout décideur. Ce contexte crée de l'incertitude et de la complexité pour les dirigeants qui ne doivent pas seulement s'adapter aux mutations de leur environnement, mais les maîtriser et savoir les influencer pour en tirer le meilleur parti.

En miroir, l'identification et la protection de la ressource informationnelle stratégique par la mise en œuvre d'une structure organisationnelle cohérente permettent aux dirigeants une anticipation des évènements susceptibles de se manifester dans leur environnement. Cette anticipation est le facteur clé permettant d'initier une réflexion stratégique génératrice d'avantages concurrentiels durables et sources de futurs profits potentiels.

Comme il a été décrit dans notre mémoire, les enjeux stratégiques de la guerre informationnelle ne sont plus à démontrer, ils répondent à des besoins primaires de toute démarche d'intelligence économique, et révèlent non seulement des techniques offensives permettant à l'entreprise d'initier des actions volontaristes de déstabilisation de ses concurrents et défensives en préservant son patrimoine immatériel de toutes formes de prédations extérieures.

L'étude bibliographique de l'intelligence économique est riche de nombreux ouvrages proposant des grilles d'identification et d'analyse de l'information, mais il s'avère que les outils exposés sont souvent redondants et insuffisamment exhaustifs dans leur contenu.

En conséquence, l'approche retenue est de mettre à disposition des dirigeants un autodiagnostic exhaustif en termes de critères retenus, ainsi que de domaines diagnostiqués. Notre parti pris a été notamment de s'attacher à interroger l'entreprise dans sa perception à décrire et identifier sa propre ressource informationnelle par l'intermédiaire d'un critère tel « la culture interne de l'entreprise ». Bien conscients des limites inhérentes à la ressource « temps » des dirigeants, un autodiagnostic « simplifié » est proposé sans pour autant se départir de l'exhaustivité des thèmes abordés.

Notre recherche bibliographique relative au domaine de l'intelligence économique nous a interrogés sur le manque observé en termes de priorisation structurée des actions. En conséquence, il a été initié une proposition de référentiel de réponses à des incidents et menaces sur la base du référentiel MITRE Att&CK (« Adversarial Tactics, Techniques and Common Knowledge) utilisé par les acteurs de la menace dans le monde numérique. L'objectif de notre démarche est de fournir un référentiel structuré de tactiques, techniques et procédures visant à répondre aux attaques informationnelles dans le cadre plus général de l'intelligence économique et non restreinte à l'environnement numérique.

Dans un souci de démarche globale, diagnostic, réponse structurée à des menaces, et priorisation des actions à entreprendre, un modèle de fiches pratiques et synthétiques est mis à disposition des décideurs avec la volonté de « pointer du doigt » deux manques des fiches pratiques préexistantes : le coût et la ressource qui sont associés à ces mesures.
En termes de perspectives, il parait évident que la menace informationnelle est en constante évolution, et nécessite donc une adaptation en continu. L'intégration de l'intelligence artificielle et du « machine learning » s'imposeront comme des outils dans le futur pour faire face aux menaces de désinformation

en ligne. Par contre, elle devra toujours être associée à une action humaine pour en analyser les contours et contextes.

S'intéresser à la « guerre informationnelle » doit s'inscrire dans un processus de suivi régulier et proactif des nouvelles technologies et domaines du numérique. L'émergence future d'un monde virtuel fictif (« metaverse ») composé d'espaces virtuels et partagés (utilisation d'avatars, autonomie des univers..) permettra l'accès à de nombreuses activités et notamment commerciales. En conséquence, il parait évident à minima que des processus de veille spécifiques soient initiés afin ne pas être à « la traîne » de cette révolution numérique.

Annexes et bibliographie

7.1. Questionnaire détaillé

1. L'IDENTIFICATION DE LA RESSOURCE INFORMATIONNELLE STRATÉGIQUE			
1.1. LA CULTURE INTERNE DE L'ENTREPRISE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Est-ce que l'information dans l'entreprise est perçue comme un facteur d'action ?		
2	Est-ce que l'information dans l'entreprise est perçue comme un instrument de pouvoir ?		
3	Existe-t-il un échange de connaissances et un partage d'expériences au sein de l'entreprise ?		
4	Est-ce que tous les acteurs de l'entreprise participent au développement, à l'enrichissement et à la protection de la mémoire de l'entreprise ?		
5	Portez-vous une attention particulière à la discrétion et à la confidentialité dans l'entreprise ?		
6	Le personnel de votre entreprise est-il sensibilisé au problème de protection de l'information ?		
7	Le personnel de votre entreprise est-il sensibilisé aux notions de l'éthique et de la déontologie ?		
8	Acceptez-vous l'échange d'informations avec l'environnement de votre entreprise (clients, fournisseurs, concurrents…) ?		
9	Portez-vous un intérêt à s'adapter aux habitudes culturelles de l'environnement de votre entreprise ?		
10	Existe-t-il un état d'esprit favorable au changement et à la nouveauté ?		
11	Entretenez-vous des liens avec des acteurs de culture différente ?		
12	Tenez-vous à connaître les cultures des partenaires et clients ?		
13	Pensez-vous que vous maîtrisez la communication dans un contexte culturel différent ?		
14	Pensez-vous être capable de maîtriser le risque des chocs culturels avec vos partenaires/clients ayant des cultures différentes de la vôtre ?		
15	Prenez-vous suffisamment de recul par rapport à une situation de confrontation culturelle ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
1.2. LE TRAITEMENT INTERNE DE L'INFORMATION			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Procédez-vous à une description fine de la demande informationnelle, l'enjeu du problème décisionnel et le contexte qui l'a engendré ?		
2	Procédez-vous à une actualisation régulière de l'identification des besoins de l'information ?		
3	Procédez-vous à une traduction du problème décisionnel en questions de recherche d'informations ?		
4	Procédez-vous à la vérification de la bonne compréhension de la demande informationnelle ?		
5	Procédez-vous à l'élaboration d'un plan de recherche d'informations pour chaque besoin informationnel ?		
6	Existe-t-il une procédure d'évaluation des sources d'informations (feed-back) ?		
7	Portez-vous un intérêt particulier à la collecte d'informations à caractère anticipatif ?		
8	Existe-t-il une étape, clairement identifiée, d'analyse et de synthèse des informations traitées ?		
9	Existe-t-il une procédure d'évaluation de la qualité des informations collectées ?		
10	Lorsque vous collectez une information stratégique, procédez-vous à une sauvegarde dans une mémoire de l'entreprise ?		
11	Procédez-vous à une actualisation des informations de la mémoire de l'entreprise ?		
12	Les destinataires des informations pertinentes sont-ils identifiés ?s		
13	Est-ce que les délais de diffusion des informations sont respectés ?		
14	Les informations de la mémoire de l'entreprise sont-elles sécurisées ?		
15	Existe-t-il une évaluation et un contrôle du processus de veille ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
1.3. IDENTIFICATION DE L'INFORMATION STRATÉGIQUE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Existe-t-il une vision stratégique au sein de l'entreprise ?		
2	Procédez-vous à une capitalisation des connaissances stratégiques dans votre entreprise ?		
3	La réflexion stratégique est-elle alimentée par les indicateurs informationnels en provenance du veilleur ?		
4	Préservez-vous une vigilance stratégique permanente pour être plus clairvoyant et à l'écoute de ce qui se prépare et qui pourra un jour vous nuire ?		
5	Existe-t-il une coordination des stratégies des différentes unités de l'entreprise ?		
6	Procédez-vous à une formalisation de la réflexion stratégique ?		
7	Les stratégies que vous mettez en place sont-elles originales par rapport à celles des concurrents ?		
8	Avez-vous identifié la sensibilité des informations en fonction du préjudice qu'engendreraient leur divulgation, leur perte ou leur destruction pour la vie de l'entreprise ?		

9	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer un dommage pour l'activité de la structure ou le déroulement d'un projet ?		
10	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer un impact financier ou technique ?		
11	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer un impact sur le personnel ?		
12	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer un impact en matière d'image et de réputation ?		
13	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer une incidence sur la confiance des actionnaires ou des banques ?		
14	La perte, la destruction ou la divulgation de cette information stratégique est-elle de nature à engendrer une perte de confiance d'un client ou d'un partenaire important ?		
15	Les droits d'accès à l'information stratégique sont-ils strictement régis dans votre entreprise (très limités, limités, restreints) ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
1.4. RÉSEAU ET INFLUENCE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	La structure organisationnelle de l'entreprise permet-elle le travail en mode réseau ?		
2	L'entreprise est-elle inscrite dans une logique de réseau interne (interactivité entre les membres de l'entreprise ?		
3	L'entreprise est-elle inscrite dans une logique de réseau externe pour renforcer la synergie entreprise-environnement ?		
4	Existe-t-il des modalités d'animation et d'évaluation des réseaux internes que vous mettez en place ?		
5	Existe-t-il des modalités d'animation et d'évaluation des réseaux externes que vous mettez en place ?		
6	Cherchez-vous à créer, entretenir ou participer à des réseaux hors de votre entreprise afin de disposer de sources et de moyens de diffusion d'informations utiles et diversifiés ?		
7	L'entreprise adhère-t-elle à des associations professionnelles permettant de faire entendre sa voix ?		
8	L'entreprise conduit-t- elle ou participe-t-elle à des actions à caractère sociétal (adhésion à des associations sportives, culturelles, humanitaires) ?		
9	Menez-vous des actions d'influence pour préserver et renforcer les intérêts de votre entreprise (organismes de normalisation, décideurs publics locaux, ministères, ONG) ?		
10	Avez-vous une politique de communication pour promouvoir votre entreprise et faire valoir les performances de ses produits ?		
11	Etes-vous prêt à faire appel à un cabinet de lobbying pour défendre et promouvoir votre entreprise ?		
12	Existe-t-il une implication directe de la direction générale dans les actions d'influence?		
13	Votre entreprise a-t-elle les moyens de rétablir sa réputation en cas d'attaque informationnelle ?		
14	Accordez-vous un intérêt particulier à la mise en place d'opérations de contre-influence afin de se protéger des actions de déstabilisation ou de manipulation ?		
15	La stratégie que vous développez est-elle de nature de surprise ou d'attaque de front ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
1.5. LA VEILLE INFORMATIONNELLE ÉCONOMIQUE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Connaissez-vous votre capital information déjà disponible ?		
2	Avez-vous identifié précisément votre besoin en information (priorisation des besoins) ?		
3	Avez-vous une structure interne de veille économique ?		
4	Vous appuyez-vous sur des prestataires extérieurs ?		
5	Suivez-vous régulièrement l'environnement économique du secteur d'activité de l'entreprise ?		
6	Surveillez-vous les acteurs clés de votre domaine (grands groupes, PME…) ?		
7	Avez-vous défini l'échelle géographique de votre recherche ? (locale, régionale, nationale, européenne, internationale) ?		
8	Suivez-vous régulièrement la législation et la réglementation applicables à l'entreprise ?		
9	Etes-vous dotés d'outils de veille adaptés à la taille et aux besoins de votre entreprise ?		
10	Diversifiez-vous vos sources d'informations ? (moteurs de recherche, blogs, forums, réseaux sociaux…) ?		
11	Suivez-vous régulièrement l'action des associations, des « think tanks », des ONG s'intéressant à votre secteur d'activité ou à votre entreprise ?		
12	Suivez-vous régulièrement l'évolution des besoins et des atteintes de vos clients ?		
13	Suivez-vous régulièrement vos concurrents (nouveaux produits, projet de délocalisation, croissance externe) ?		
14	Avez-vous des sources d'informations internes et savez-vous les valoriser (savoir-faire du personnel , rapports de SAV..) ?		
15	Développez-vous des partenariats avec des entreprises proches géographiquement et/ou de en termes de secteur d'activité (échange d'informations, participation collective à des salons) ?		

	RÉSULTAT		
	SCORING = 0 < **x** < 15		
	2. LA PRÉSERVATION DE LA RESSOURCE INFORMATIONNELLE DE L'ENTREPRISE		
	2.1. ÉVITER OU GÉRER LA PERTE D'UNE COMPÉTENCE CLÉ		
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Avez-vous cartographié les compétences clés en anticipant la stratégie de développement de l'entreprise et les perspectives du marché ?		
2	Développez-vous une veille sur les offres d'emploi du secteur, notamment de la concurrence ?		
3	Développez-vous une veille sur le climat social interne ?		
4	Gardez-vous à l'esprit que le cloisonnement des missions, des activités et des compétences internes accroît les risques de départ ?		
5	Favorisez-vous, par la formation interne, le partage des bonnes pratiques et des compétences ?		
6	Etablissez-vous en amont les schémas d'intervention en cas de vacance d'un poste (personnes relais, délégations de décision, de signature…) ?		
7	Fidélisez-vous les compétences clés par une politique de gestion des ressources humaines personnalisée (motivation, intéressement, actionnariat…) ?		
8	Profitez-vous des entretiens annuels afin de réévaluer les salaires/primes, les conditions de travail, les projets souhaités… ?		
9	Formalisez-vous dans les contrats de travail des clauses de confidentialité (durée, champs d'application…), de loyauté (non concurrence, l'espace géographique et la contrepartie financière, afin d'éviter son annulation), de dédit-formation (remboursement de la formation par le collaborateur) ?		
10	Souscrivez-vous, le cas échéant, pour une compétence rare, une police d'assurance « personne clé » ?		
11	Analysez-vous à l'annonce du départ l'impact potentiel de la perte subie en termes d'image et/ou de perte d'informations stratégiques ?		
12	Sécurisez-vous le départ pour que le préavis ne soit pas source de problèmes pour l'entreprise (procédures informatiques, badges d'accès, clefs, téléphones..) ?		
13	Mesurez-vous après le départ l'impact de la perte subie (quel concurrent a bénéficié de la compétence-clé ? Y a-t-il eu divulgation des informations stratégiques ?)		
14	En interne, identifiez-vous après le départ « le manque » observé et déterminez-vous l'organisation permettant d'y pallier au mieux ?		
15	Effectuez-vous un retour d'expérience en interne pour comprendre les raisons de cette perte de compétence clé ?		
	RÉSULTAT		
	SCORING = 0 < **x** < 15		
	2.2. PROTÉGER SON SAVOIR ET SES IDÉES		
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Identifiez-vous, parmi les différents titres de propriété intellectuelle (brevets, marques, dessins et modèles, droits d'auteur…) ceux qui sont les mieux adaptés pour valoriser vos innovations, vos produits et créations immatérielles ?		
2	Avant de déposer une marque ou un brevet, vérifiez-vous auprès de l'Institut National de la Propriété Industrielle (INPI) la disponibilité du droit à protéger pour s'assurer du caractère nouveau de la création (recherches d'antériorité) ?		
3	Examinez-vous la nécessité de vous faire assister d'un conseil en propriété intellectuelle ?		
4	Identifiez-vous les marchés (national, communautaire, international), présents et futurs, sur lesquels protéger ses droits ?		
5	Enregistrez-vous vos droits auprès des offices compétents (INPI, Office de l'Union Européenne pour la Propriété Intellectuelle…) ?		
6	Faites-vous enregistrer les noms de domaine liés aux titres et à l'activité commerciale auprès de l'agence française pour le nommage sur internet en coopération (Afnic) ?		
7	Une veille, notamment sur internet, est-elle mise en place, afin de détecter et de se prémunir des contrefaçons ?		
8	En cas de suspicion de contrefaçon, avez-vous déjà déposé une demande d'intervention auprès des Douanes pour mettre en retenue ces produits ?		
9	Protégez-vous vos créations par une confidentialité stricte des documents relatifs aux droits et aux produits (clauses de confidentialité, protection physique et numérique des documents…) ?		
10	Avez-vous déjà été assisté par un avocat ou un conseil en propriété intellectuelle dans le cas de l'utilisation par un tiers d'un droit détenu par l'entreprise ?		
11	Avez-vous déjà fait opposition auprès de l'INPI dans le cas de l'utilisation par un tiers d'un droit détenu par l'entreprise ?		
12	Avez-vous déjà communiqué aux autorités compétentes (Douanes) les informations dont dispose l'entreprise sur la contrefaçon (circuit de fraude, identité des contrefacteurs, caractéristiques des marchandises contrefaites…) ?		
13	Avez-vous déjà intenté une action en justice contre le présumé contrefacteur afin de faire cesser l'infraction et d'obtenir des dommages et intérêts ?		
14	Gardez-vous à l'esprit que le dépôt d'un brevet peut renseigner sur l'existence d'une compétence clé ?		
15	Établissez-vous une stratégie interne en matière de propriété intellectuelle ?		
	RÉSULTAT		
	SCORING = 0 < **x** < 15		

2.3. ACCUEILLIR ET ENCADRER DU PERSONNEL TEMPORAIRE			
#	QUESTION	NON (0)	OUI (1)
1	Existe-t-il un processus en amont visant à bien connaître le parcours du futur personnel temporaire avant qu'il n'arrive ?		
2	Les informations relatives à la mission du personnel temporaire sont-elles bien partagées par tous les services concernés (RH, SSI, sécurité…°) ?		
3	Une personne de l'entreprise est-elle responsable de l'encadrement du personnel temporaire tout au long de sa mission dans l'entreprise ?		
4	Existe-t-il un répertoire tenu à jour des personnels non permanents (nom du responsable de l'encadrement, date de début et de fin de la mission…) ?		
5	Est-il prévu dans le contrat ou la convention de mise à disposition de personnel une clause de confidentialité spécifiant l'interdiction formelle de toute diffusion d'informations relatives à l'entreprise ?		
6	Le personnel temporaire est-il sensibilisé dès son arrivée aux mesures de sécurité exigées par l'entreprise ?		
7	Faites-vous signer dès son arrivée au personnel temporaire le règlement intérieur et la charte informatique ?		
8	Imposez-vous le port d'un badge spécifique et apparent pour les personnels temporaires ?		
9	Apportez-vous une attention particulière aux informations figurant dans les documents produits par les personnels temporaires (rapport de stage, mémoire, livrable…) ?		
10	Saisissez-vous rapidement les services de police ou de gendarmerie compétents en cas de malveillance suspecte ?		
11	Suivez-vous le parcours des stagiaires durant quelques mois après leur départ ?		
12	Autorisez-vous l'accès aux systèmes d'information qu'à partir d'équipements fournis par l'entreprise, et à l'aide d'un identifiant personnel et tracé ?		
13	Limitez-vous l'accès aux ressources informatiques et aux informations nécessaires et en relation directe avec leur sujet de travail ?		
14	Clôturez-vous les comptes informatiques des personnels temporaires immédiatement après la fin de leur contrat pour l'entreprise ?		
15	En présence de personnel temporaire, n'évoquez-vous que des sujets se rapportant à leur mission ?		
RÉSULTAT			
SCORING = 0 < x < 15			
2.4. PROTECTION DES LOCAUX			
#	QUESTION	NON (0)	OUI (1)
1	Existe-t-il dans votre entreprise un responsable sûreté chargé de la rédaction des procédures et du contrôle de la mise en œuvre ?		
2	Prenez-vous en compte les risques liés à l'environnement immédiat : le voisinage, les bâtiments adjacents…. ?		
3	Identifiez-vous les flux d'entrées et de sorties au sein de l'entreprise (personnes, informations, marchandises….) ?		
4	Hiérarchisez-vous les zones à protéger en fonction des risques, des acteurs, ou du fonctionnement de l'entreprise ?		
5	Adaptez-vous des mesures de sécurité en fonction des zones à protéger ?		
6	Existe-t-il une réglementation d'accès aux différentes zones en fonction des nécessités réelles de chacun ?		
7	Existe-t-il un journal des incidents, des reports et alertes ?		
8	Existe-t-il une sensibilisation régulière des personnels aux règles de sécurité du site ?		
9	Existe-t-il des formations adaptées aux règles de sécurité du site en y associant les prestataires de service et les partenaires aux dispositifs internes de protection des locaux ?		
10	Evaluez-vous périodiquement la performance du système de contrôle d'accès (audits internes, exercices, tests d'intrusion, délais d'intervention…) ?		
11	Les systèmes de sûreté (contrôle d'accès, détection d'intrusion, vidéosurveillance) sont-ils centralisés au sein du poste central de sécurité ?		
12	Une gestion rigoureuse des clés et des badges d'accès est-elle prévue ?		
13	Le périmètre de l'entreprise est-il délimité en utilisant une signalétique appropriée (panneau de l'entreprise, propriété privée…) ?		
14	Existe-t-il un système de détection des intrusions (barrières anti-intrusion…° ?		
15	L'entreprise est-elle équipée d'un système de vidéosurveillance ?		
RÉSULTAT			
SCORING = 0 < x < 15			
2.5. ENCADRER DES VISITEURS			
#	QUESTION	NON (0)	OUI (1)
1	Impliquez-vous l'ensemble du personnel lors de visites sensibles (regain de vigilance…) ?		
2	Adoptez-vous des schémas de sécurité conformes à l'objet/ la nature de la visite ou du visiteur ?		
3	Connaissez-vous avant même la visite, l'identité, les coordonnées et la fonction des visiteurs ? (N'acceptez-vous que ceux qui sont déclarés) ?		
4	Élaborerez-vous formellement une procédure d'accueil des visiteurs quels qu'ils soient ?		
5	L'ensemble du personnel est-il informé de la procédure d'accueil des visiteurs ?		
6	Vérifiez-vous strictement l'identité des visiteurs à leur arrivée ?		
7	Un badge d'accueil distinctif et dont le port est obligatoire est-il fourni aux visiteurs ?		
8	Des lieux spécifiquement dédiés à l'accueil des visiteurs sont-ils prévus(stationnement, réception) ?		
9	Définissez-vous précisément les informations qui pourront être évoquées au cours de la visite ?		
10	Définissez-vous un parcours de visite (circuit de notoriété) excluant les zones les plus confidentielles ?		
11	Accompagnez-vous les visiteurs, dans la mesure du possible en permanence, de leur arrivée à leur départ ?		

12	Enregistrez-vous les horaires d'entrées et de sorties des visiteurs (conservation de la trace) ?		
13	Encadrez-vous strictement l'utilisation d'outils numériques (smartphones, appareils photo, lunettes ou montres connectées, clés USB …) ?		
14	Prévoyez-vous un ordinateur dédié, non connecté au réseau, permettant de recevoir les supports amovibles des visiteurs ?		
15	Etes-vous vigilants aux questionnements trop intrusifs dont pourraient faire preuve certains visiteurs ?		
	RÉSULTAT		
	SCORING = 0 < **x** < 15		
	3. LES MESURES ORGANISATIONNELLES DE PROTECTION DE L'INFORMATION		
	3.1. MAÎTRISER SA COMMUNICATION EXTERNE		
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Votre entreprise est-elle exposée médiatiquement ?		
2	Votre établissement peut-il faire l'objet d'une campagne de dénigrement de la part de groupes de pression ?		
3	Un changement dans votre production (délocalisation, changement de sous-traitant…) est-il susceptible d'affecter l'image de votre entreprise ?		
4	Évaluez-vous votre entreprise au sein de votre clientèle ?		
5	L'entrée dans votre capital d'un acteur véhiculant une image négative est-elle susceptible d'affecter votre réputation ?		
6	Pour préserver votre image, vous attachez vous à une charte d'engagement éthique ?		
7	Utilisez-vous une charte graphique pour vos documents ?		
8	Demandez-vous à tous les employés de l'entreprise de faire valider, préalablement et systématiquement, auprès de sa Direction, tout contact avec un journaliste, un analyste financier… ?		
9	En cas d'entretien avec un média externe, demandez-vous à vos collaborateurs de toujours s'interroger si les questions sont légitimes et si elles s'inscrivent dans la stratégie de communication ?		
10	En cas d'entretien avec un média externe, demandez-vous à l'avance la liste des questions ?		
11	En cas d'entretien avec un média externe, demandez-vous de pouvoir relire les réponses communiquées avant publication par celui-ci ?		
12	Sur les supports de communication (cartes de visite, signature électronique….), n'indiquez-vous que ce qui est strictement nécessaire à la relation professionnelle ?		
13	Sensibilisez-vous les collaborateurs aux risques de sollicitations urgentes , inhabituelles et ne respectant pas les procédures de communication ?		
14	Une procédure d'urgence de communication en cas d'incident est-elle mise en place dans l'entreprise ?		
15	Vos collaborateurs s'assurent-ils de la légitimité des démarches d'audit et contrôles (identités, mandats…) ?		
	RÉSULTAT		
	SCORING = 0 < **x** < 15		
	3.2. SE DÉPLACER À L'ETRANGER		
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Lors de déplacements à l'étranger, vous renseignez-vous sur les législations locales en matière de chiffrement des données ?		
2	Préparez-vous pour vos salariés des numéros de téléphone d'urgence (assistance, et services diplomatiques) ?		
3	Vos salariés n'emportent-ils que des documents indispensables à la mission ?		
4	Les données sensibles transportées par vos salariés sont-elles chiffrées ?		
5	En cas de sensibilité particulière du déplacement, vos salariés disposent-ils d'un ordinateur portable et d'un téléphone dédiés ?		
6	Lors des déplacements sensibles, les ports USB, les connexions Wifi et Bluetooth des ordinateurs portables sont-elles désactivées ?		
7	Demandez-vous à vos salariés de ne pas laisser leurs données sensibles dans le coffre-fort de leur hôtel ?		
8	Interdisez-vous l'utilisation du WIFI des hôtels à vos salariés en déplacement ?		
9	Vos salariés évitent-ils les sollicitations impromptues demandées à titre amical ?		
10	Vos salariés évitent-ils les excès de toute nature susceptibles d'être utilisés à son encontre ?		
11	Evitez-vous les signes d'appartenance ou d'identification à une entreprise ?		
12	Vos salariés sont-ils sensibilisés à ne pas s'engager dans des conversations sensibles ou confidentielles dans les chambres d'hôtels, chez un particulier ou dans les espaces publics ?		
13	Dans les salons et réunions internationaux, maîtrisez-vous l'information à diffuser (faux clients, et sollicitations multiples) ?		
14	Vos salariés sont-ils interdits d'utiliser des supports informatiques remis lors de leurs voyages (clés USB, goodies…) ?		
15	En cas de faits étonnants, vos salariés rendent-ils compte à leur Direction (rapport d'étonnement)?		
	RÉSULTAT		
	SCORING = 0 < **x** < 15		
	3.3. PARTICIPER À UN SALON PROFESSIONNEL		
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Définissez-vous les informations qui pourront être diffusées ou non ?		
2	Préparez-vous avec vos salariés les éléments de langage sur les sujets délicats (innovation, savoir-faire..) ?		
3	Désignez-vous un responsable en charge du matériel sensible lors du montage et du démontage du stand lors des périodes exposées ?		
4	Identifiez-vous par badge les animateurs du stand ?		
5	Choisissez-vous l'emplacement de votre stand en fonction de la concurrence ?		

6	Vous assurez-vous que le stand initialement proposé n'est pas déplacé au dernier moment ?		
7	Prévoyez-vous des vitrines fermées à clé pour stocker les matériels sensibles ?		
8	Envisagez-vous une zone permettant des échanges en toute discrétion ?		
9	Sensibilisez-vous vos collaborateurs sur des risques de manipulation (flatterie, partage d'un intérêt commun, fausse vérité, information gratuite…°) ?		
10	Préparez-vous des réponses adaptées en cas de demandes par la presse ?		
11	Préparez-vous des plaquettes de plusieurs niveaux d'information successifs en fonction du type d'interlocuteurs ?		
12	Préparez-vous un ordinateur uniquement dédié aux prestations pour le salon et dénué de données sensibles ?		
13	Verrouillez-vous tous les ports USB des ordinateurs possédant des données USB ?		
14	Mettez-vous en place une déchiqueteuse pour détruire tous les documents de travail (schémas, devis…) ?		
15	Demandez-vous à vos salariés de faire un retour d'expérience concernant le salon (rapport d'étonnement si nécessaire)		
RÉSULTAT			
SCORING = 0 < **x** < 15			

3.4. GÉRER SES ARCHIVES ET SES REJETS

#	QUESTION	NON (0)	OUI (1)
1	Mettez-vous en place une solution de suivi, un plan de classement et d'archivage spécifique pour les supports d'information dont le contenu est stratégique ?		
2	Formez-vous vos collaborateurs à une gestion précise (sauvegarde, niveau de sensibilité, durée de vie…) des documents qu'ils créent (notes manuscrites, fichiers numériques, bordereaux..) ?		
3	Mettez-vous en place une procédure de traçabilité de la consultation des différentes formes d'archives ?		
4	En cas d'externalisation des archives numériques, encadrez-vous systématiquement le contrat avec le prestataire ?		
5	Insérez-vous dans les contrats de location de matériels informatiques des clauses spécifiques prévoyant la conservation des disques durs ou leur destruction sécurisée ?		
6	Fournissez et gérez-vous les supports d'affichage amovibles vérifiés (clé USB, disque externe…°) ?		
7	Conservez-vous les archives papier et numériques dans des locaux sécurisés et adaptés (restriction d'accès, protection contre les sinistres…) ?		
8	Archivez-vous les données stratégiques avec des précautions particulières (coffre fort, chiffrement…) ?		
9	Testez-vous régulièrement l'intégrité des documents numériques archivés ?		
10	Définissez-vous une politique interne de gestion des déchets professionnels (yc dans le domaine du télétravail) ?		
11	Sensibilisez-vous les collaborateurs au fait qu'une simple suppression de données ne constitue pas une réelle destruction ?		
12	Mettez-vous à disposition un broyeur à coupe croisée pour détruire de manière sécurisée les documents sensibles ?		
13	Installez-vous sur chaque poste de travail un logiciel d'effacement sécurisé ?		
14	Détruisez ou effacez-vous de façon sécurisée les mémoires internes des équipements informatiques en fin de vie ou de contrat ?		
15	Détruisez-vous de façon sécurisée les prototypes de matériaux innovants mis au rebut afin d'éviter la rétro-ingénierie ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			

3.5. LES ESCROQUERIES DITES « AU PRÉSIDENT » OU FOVI (FAUX ORDRES DE VIREMENT INTERNATIONAL)

#	QUESTION	NON (0)	OUI (1)
1	Sensibilisez-vous régulièrement tout le personnel (yc les stagiaires, les nouveaux arrivants…) à ce type d'escroquerie ?		
2	Expliquez-vous les principales vulnérabilités associées à l'usage des réseaux sociaux et la nécessité de ne pas mettre en avant des informations utilisables dans le cadre d'un FOVI (informations comptables…) ?		
3	Mettez-vous en place des procédures de vérifications et de signatures multiples pour les paiements internationaux ?		
4	Respectez-vous les procédures mises en place malgré les pressions d'un interlocuteur souhaitant un paiement dans l'urgence ?		
5	Exigez-vous une solution écrite via un courriel professionnel afin de pouvoir le vérifier ?		
6	Etes-vous attentifs aux demandes inhabituelles de transmission de nouvelles coordonnées bancaires (remontée d'informations inquiétantes) ?		
7	Redoublez-vous de vigilance sur les périodes de congés scolaires, les jours fériés, les vendredis soir, les week-ends, et les périodes de remplacement ?		
8	Vous êtes-vous rapprochés de votre organisme bancaire pour connaître les procédures applicables ?		
9	En cas d'escroquerie, êtes-vous en mesure d'identifier immédiatement les virements exécutés ou les demandes en instance ?		
10	En cas d'escroquerie, demandez-vous le blocage des coordonnées bancaires dans les applications métiers ?		
11	En cas d'escroquerie, si le paiement n'est pas encore intervenu, suspendez-vous immédiatement la demande de paiement ?		
12	En cas d'escroquerie, si le paiement est déjà intervenu, demandez-vous le blocage ou le retour des fonds auprès de l'instance bancaire ?		
13	En cas d'escroquerie, déposez-vous plainte auprès des services de police ?		
14	Avez-vous déjà été approché dans le cadre d'une fraude au « changement de RIB » ?		
15	Avez-vous déjà été approché dans le cadre d'une fraude au « faux technicien » ?		

RÉSULTAT			
SCORING = 0 < **x** < 15			
4. LA MAÎTRISE DU RISQUE NUMÉRIQUE			
4.1. LA POLITIQUE DE SÉCURITÉ INFORMATIQUE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Votre entreprise s'est-elle dotée d'une politique de sécurité informatique ?		
2	Avez-vous désigné une personne responsable de la mise en place de la politique de sécurité informatique ?		
3	Avez-vous défini le périmètre et les objectifs de la politique de sécurité informatique ?		
4	**Avez-vous effectué une analyse de l'existant,** matériel et logiciel ?		
5	Avez-vous effectué une analyse des risques informatiques (au regard du préjudice possible et de la probabilité d'occurrence de l'incident) ?		
6	**Avez-vous déterminé les moyens nécessaires** pour la réduction des risques et la prise en charge des incidents ?		
7	Avez-vous élaboré une charte informatique à destination des collaborateurs ?		
8	Avez-vous communiqué sur la politique de sécurité informatique auprès de l'ensemble de votre entreprise ?		
9	Avez-vous déterminé précisément vos besoins précis en externalisation informatique (« cloud computing », plateforme logicielle à distance…) ?		
10	Hiérarchisez-vous les objectifs de sécurité de l'entreprise (disponibilité du site internet, hébergement sur les serveurs dédiés…) ?		
11	Demandez-vous aux prestataires répondant aux appels d'offres un Plan d'assurance sécurité (Pas) ?		
12	Etes-vous sensibilisé aux risques liés à la perte d'informations lors d'hébergement mutualisé ?		
13	Etes-vous sensibilisé aux risques liés à la perte de confidentialité des données dans le cadre d'un cloud computing?		
14	Etes-vous sensibilisé aux risques juridiques liés à l'incertitude sur la localisation des données dans le cadre d'un cloud computing?		
15	Etes-vous sensibilisé aux risques liés à l'irréversibilité des contrats dans le cadre d'un cloud computing?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
4.2. PROTÉGER SON SYSTÈME D'INFORMATION			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Tenez-vous à jour la liste précise de tous les équipements informatiques de l'entreprise qui peuvent se connecter au réseau (postes utilisateurs, serveurs, imprimantes…) ?		
2	Identifiez-vous nommément chaque utilisateur ?		
3	Supprimez-vous minutieusement les comptes anonymes et génériques ?		
4	Attribuez-vous des droits d'accès (répertoires, calendriers..) de façon graduée et adaptée aux besoins ?		
5	Actualisez-vous les droits d'accès lors des arrivées, des départs et des mouvements internes ?		
6	Dédiez-vous les comptes d'administration à ces seules tâches ?		
7	Limitez-vous drastiquement le nombre d'utilisateurs disposant de droits d'administrateurs ?		
8	Vous assurez vous de la suppression effective des droits d'accès au système d'information lors d'un collaborateur ?		
9	Mettez-vous en place une passerelle d'accès à internet sécurisée à travers la mise en place d'un pare-feu ?		
10	Cloisonnez-vous les différents services au sein du réseau (isolation des services exposés à internet du SI) ?		
11	Cloisonnez-vous les fonctions d'administration du reste du système d'information ?		
12	Vérifiez-vous qu'aucun équipement connecté au réseau interne ne puisse être administré via internet ?		
13	Renouvelez-vous régulièrement les identifiants et mots de passe configurés sur tous les équipements ?		
14	Avez-vous supprimé les prises d'accès physique au réseau interne accessible à tous (salle d'attente, de réunion…°?		
15	Limitez-vous la télémaintenance ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
4.3. PROTÉGER SON POSTE DE TRAVAIL INFORMATIQUE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Faites-vous appliquer une politique de choix de mots de passe robustes ?		
2	Demandez-vous à vos salariés de définir un mot de passe unique et personnel pour chaque usage ?		
3	Mettez-vous à jour régulièrement le système d'exploitation et les logiciels ?		
4	Téléchargez-vous les installateurs de logiciels uniquement depuis les sites de leurs éditeurs (vérification de leur authenticité) ?		
5	N'installez-vous que le strict nécessaire sur les postes de travail de vos collaborateurs ?		
6	Limitez-vous les logiciels installés et les modules optionnels des navigateurs sur les postes de travail de vos collaborateurs ?		
7	Utilisez-vous un pare-feu local et un anti-virus ?		
8	Utilisez-vous un gestionnaire de mot de passe pour leur stockage (mot de passe robuste) ?		
9	Désactivez-vous les exécutions automatiques sur les postes de travail de vos collaborateurs ?		
10	Chiffrez-vous les partitions où sont stockées les données utilisateur ?		
11	Désactivez-vous les ports USB non utilisés pour la connexion des périphériques ?		

12	Protégez-vous l'accès aux informations sensibles à l'aide d'un système de contrôle d'accès adapté (conteneurs chiffrés..) ?		
13	Effectuez-vous régulièrement des sauvegardes de données ?		
14	Avez-vous procédé à une sensibilisation de vos salariés concernant les courriels suspects ?		
15	Les salariés bénéficiant de droits d'administrateur utilisent-ils des comptes séparés pour la navigation sur internet ?		
4.4. LA SÉCURISATION NUMERIQUE DU TRAVAIL NOMADE			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Avez-vous défini une politique de mise à disposition d'outils nomades maîtrisée afin d'éviter les écueils d'un recours à l'utilisation d'outils personnels ?		
2	Veillez-vous à ce que vos salariés n'utilisent leurs appareils nomades personnels uniquement à des fins professionnelles ?		
3	En plus du code PIN protégeant la carte téléphonique de vos salariés, utilisez-vous un schéma ou un mot de passe pour sécuriser l'accès au smartphone ?		
4	Vos salariés évitent-ils d'installer des applications demandant l'accès à des données sur leurs appareils nomades ?		
5	Vos salariés connaissent-ils les fonctions de sécurité de leurs téléphones portables ?		
6	Avez-vous installé un filtre de confidentialité sur les écrans des ordinateurs portables et des smartphones de vos collaborateurs ?		
7	Vos salariés évitent-ils de transporter des données sensibles lors de leurs déplacements quotidiens ?		
8	Une solution de chiffrement (conteneur chiffré ou clé USB sécurisée) a-t-elle été prévue ?		
9	Le VPN est-il privilégié en cas d'utilisation des appareils nomades lors du travail à distance ?		
10	Vos salariés désactivent-ils les fonctions WIFI/Bluetooth de leurs appareils nomades dans les transports en commun et les espaces publics ?		
11	Vos salariés privilégient-ils les prises secteurs pour rechercher leurs appareils nomades plutôt que les prises USB afin d'éviter le risque de « juice-jacking » (aspiration des données) ?		
12	Vos salariés s'assurent-ils de ne jamais laisser leurs outils de travail (Ordinateurs…) sans surveillance ?		
13	Lors des stationnements en voiture, vos salariés gardent-ils toujours en leur possession leurs ordinateurs portables ou documents ?		
14	Vos salariés sont-ils sensibilisés à taper discrètement leurs identifiant et mot de passe sur leur ordinateur portable ?		
15	Dans le cas de location d'une voiture, vos salariés évitent-ils les interfaces entre le smartphone et le véhicule afin d'éviter la récupération de données ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			
4.5. VEILLE ET UTILISATION DES RÉSEAUX SOCIAUX			
#	**QUESTION**	**NON (0)**	**OUI (1)**
1	Une charte sur le bon usage des réseaux sociaux à l'attention des salariés est-elle mise en place dans votre entreprise ?		
2	En cas de mise en œuvre d'une charte de bon usage des réseaux sociaux, avez-vous informé vos salariés de son caractère juridique ?		
3	Avez-vous désigné un « community manager » suivant régulièrement les différents réseaux sociaux ?		
4	Avant toute communication sur les réseaux sociaux, veillez-vous à faire une analyse de risques simple sur les informations à communiquer ?		
5	Existe-t-il un processus de validation des communications sur les réseaux sociaux avant diffusion ?		
6	Procédez-vous à une veille régulière sur les principaux réseaux sociaux sur la publication d'informations visant à altérer la réputation de l'entreprise ?		
7	Mettez-vous en place une veille rigoureuse sur internet sur les noms de la société, de ses dirigeants et de ses marques afin de pouvoir réagir contre les dénigrements, les « cybersquats » ou toute autre action préjudiciable ?		
8	Instaurez-vous des séances de sensibilisation régulière de votre personnel concernant l'usage des réseaux sociaux ?		
9	Avez-vous expliqué à vos salariés les vulnérabilités associées à l'usage des réseaux sociaux telles que la publication de contenus relevant de son activité professionnelle ou la politique de l'entreprise ?		
10	Avez-vous expliqué à vos salariés les vulnérabilités associées à l'usage des réseaux sociaux telles que la possibilité d'être utilisés comme vecteurs de transmission de logiciels malveillants (hameçonnage)		
11	Avez-vous expliqué à vos salariés les vulnérabilités associées à l'usage des réseaux sociaux telles que les interactions sociales entre les utilisateurs connus ou inconnus (risque d'ingénierie sociale) ?		
12	Avant toute diffusion sur les réseaux sociaux, vos salariés s'assurent-ils que l'information publiée n'est pas susceptible de compromettre les intérêts de l'entreprise ?		
13	Vous êtes-vous assurés que vos salariés n'utilisent pas le même mot de passe pour accéder aux réseaux sociaux qu'aux ressources de l'entreprise ?		
14	Vous êtes-vous assurés que vos salariés évitent de communiquer des informations personnelles et professionnelles trop détaillées (missions à l'étranger, responsabilités professionnelles..°) ?		
15	Votre entreprise a-t-elle les moyens de rétablir sa réputation sur Internet en cas d'attaque ?		
RÉSULTAT			
SCORING = 0 < **x** < 15			

7.2. Fiches pratiques à destination des entreprises

En complément de la revue documentaire s'attachant à décrire les principaux concepts et outils (défensifs et offensifs) à destination des entreprises, il pourrait être intéressant développer des fiches pratiques. Ces fiches pratiques, divisés par cadrans et par thématique, permettaient, selon le niveau de maturité défini lors de l'autodiagnostic, d'entreprendre des plans d'actions spécifiques. Ainsi, nous proposons un exemple de 3 fiches pratiques décrivant :

- Le type de mesure
- En quoi cela consiste
- Les erreurs à éviter
- L'objectif visé
- Le coût estimé : cela serait calculé selon le besoin en ressource interne ou externe, l'investissement dans des softwares ou des abonnements
- La maturité nécessaire pour entreprendre cette action. En effet, la mise en place d'une cellule de renseignement complète va nécessiter plus de maturité que la mise en place d'un plan de sensibilisation / formation des salariés.

< Sensibiliser et former ses salariés >

Mesure de Cybersécurité

En quoi cela consiste ?

- Intégrer tous les salariés dans le processus de sécurité en créant une culture cybersécurité
- Partager régulièrement la Politique de Sécurité des Systèmes d'Information à l'ensemble des salariés et des tiers.
- Dispenser des formations de sécurité en présentiel et en e-learning
- Sensibiliser sur les risques liés à la cybersécurité et à la guerre économique
- Communiquer régulièrement sur les bonnes pratiques de sécurité
- Réaliser des exercices de sécurité de manière périodique (ex : exercice de phishing) et adapter la sensibilisation / formation selon les résultats

Les erreurs à éviter

- Penser que la sécurité n'est que l'affaire de la Direction des Systèmes d'Information
- Ne pas faire de suivi des résultats des exercices de sécurité
- Manquer de transparence quant à la culture de la sécurité
- Blâmer le responsable en cas d'attaque

Pour quels objectifs ?

- Réduire la probabilité des fuites de données
- Réduire la surface d'attaque
- Augmenter les remontés d'alertes

Coût estimé

€ € €

Charge estimée

Maturité nécessaire

< Mise en place de la sécurité physique >

Mesure de sécurité physique

En quoi cela consiste ?

- Dissuader : restreindre les accès aux locaux par des barrières physiques (tourniquets, équipe d'agents de sécurité)
- Détecter : mettre en place des outils de surveillance (contrôles d'accès, capteurs et caméras de surveillance)
- Atténuer : accompagner systématiquement les visiteurs, utilisation d'authentification à multiples facteurs (MFA)
- Répondre : maintenir des systèmes de communication en cas d'intrusion, verrouillage des bâtiments, appel des services compétents

Les erreurs à éviter

- Laisser des individus externes à l'entreprise évoluer librement dans les locaux
- Ne pas se doter de salariés dédiés à la sécurité physique (agents de sécurité, service des badges, agent d'accueil).
- Négliger la sécurité physique en se focalisant sur la sécurité informatique

Pour quels objectifs ?

- Protéger les salariés
- Se prémunir contre une intrusion physique
- Réduire le risque de destruction et / ou vol d'actifs

Coût estimé

€ € €

Charge estimée

Maturité nécessaire

7.3. Glossaire

Administrateur : personne physique disposant de droits privilégiés sur un système d'information, chargée des actions d'administration sur celui-ci, responsable d'un ou plusieurs domaines techniques (source ANSSI).

Anti-virus : logiciel utilitaire qui détecte et détruit les virus informatiques s'attaquant à la mémoire d'un ordinateur (source Larousse).

Brevet : le brevet protège une innovation technique, c'est-à-dire un produit ou un procédé qui apporte une solution technique à un problème donné. L'invention pour laquelle un brevet pourra être obtenu doit également être nouvelle, impliquer une activité inventive et être susceptible d'application industrielle (source INPI).

Chiffrement : procédé de cryptographie grâce auquel on rend la compréhension d'un document impossible à toute personne qui ne possède pas la clé de (dé)chiffrement (source SISSE).

Cybersquating : (accaparement de noms de domaine) action malveillante qui consiste à faire enregistrer un nom de domaine dans le seul but de bloquer toute attribution ultérieure de ce nom au profit de titulaires plus naturels ou légitimes (source ANSSI).

Circuit de notoriété : circuit préétabli permettant de faire visiter une entreprise, d'en donner une image concrète et valorisante tout en évitant les locaux sensibles (source SISSE).

Clause de confidentialité : article d'un contrat qui garantit la non-divulgation à des tiers d'informations dont la ou les personne(s) aurai(en)t connaissance par ses (leurs) fonctions . (source SISSE).

Clause de non-concurrence : La clause de non-concurrence est une clause insérée dans le contrat de travail. Elle vise à limiter la liberté d'un salarié d'exercer, après la rupture de son contrat, des fonctions équivalentes chez un concurrent ou à son propre compte. Pour être valable, la clause doit respecter certains critères (source Direction de l'information légale et administrative (Premier ministre)).

Cloud Computing : (en français, « informatique dans les nuages ») fait référence à l'utilisation de la mémoire et des capacités de calcul des ordinateurs et des serveurs répartis dans le monde entier et liés par un réseau. Les applications et les données ne se trouvent plus sur un ordinateur déterminé mais dans un nuage (*cloud*) composé de nombreux serveurs distants interconnectés (source CNIL).

Contrefaçon : La contrefaçon se définit comme la reproduction, l'imitation ou l'utilisation totale ou partielle d'une marque, d'un dessin, d'un brevet, d'un logiciel ou d'un droit d'auteur, sans l'autorisation de son titulaire, en affirmant ou laissant présumer que la copie est authentique (source INSEE).

Datasphère : Ensemble de concepts et d'implications des domaines des données informatiques, des technologies de l'information, de la cybersécurité.

Hameçonnage : (phishing) : vol d'identités ou d'informations confidentielles par subterfuge : un système d'authentification est simulé par un utilisateur malveillant, qui essaie alors de convaincre des usagers de l'utiliser et de communiquer des informations confidentielles, comme s'il s'agissait d'un système légitime.

Infogérance : l'infogérance est un service défini comme le résultat d'une intégration d'un ensemble de services élémentaires, visant à confier à un prestataire informatique tout ou partie du système d'information d'un client, dans le cadre d'un contrat pluriannuel, à base forfaitaire, avec un niveau de services et une durée définis (source AFNOR).

Ingénierie sociale : Manipulation consistant à obtenir un bien ou une information, en exploitant la confiance, l'ignorance ou la crédulité de tiers personnes(source ANSSI).

Marque : au sens de la propriété industrielle, la marque est un « signe » permettant de distinguer précisément les produits ou prestations de services d'une entreprise de ceux de ses concurrents. Le signe peut être un mot, un nom, un slogan, un logo, un dessin…ou la combinaison de ces différents éléments (source INPI).

Mot de passe robuste : la robustesse d'un mot de passe dépend en général, d'abord de sa complexité, mais également de divers paramètres. Choisir des mots de passe d'au moins 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux) (source SISSE). Le mot de passe est dans l'idéal changé tous les 90 jours et une historisation peut être mise en place afin de ne pas choisir un mot de passe identique aux 5 précédents.

Pare-feu : équipement situé entre le réseau Internet et le réseau privé d'une entreprise pour accroître la sécurité de ce dernier en filtrant le trafic en provenance ou à destination d'internet (calque de l'anglais firewall) (source Larousse).

Rançongiciel : (ou ransomware en anglais) est une contraction des mots « rançon » et « logiciel ». Il s'agit par définition d'un programme malveillant dont le but est d'obtenir de la victime le paiement d'une rançon. Forme d'extorsion imposée par un code malveillant sur un utilisateur du système (source ANSSI).

Rapport d'étonnement : compte rendu à adresser au responsable sûreté de l'entreprise relatant toute situation anormale ou inhabituelle (lors d'un déplacement ou au sein/aux abords de l'entreprise) (source SISSE).

Virtual Private Network (VPN) : (en français réseau privé virtuel) est un système permettant de créer un lien direct et sécurisé par du chiffrement entre des ordinateurs sécurisés (source SISSE).

7.4. Acronymes

AFNIC : Association Française pour le Nommage Internet en Coopération

ANSSI : Agence nationale de la sécurité des systèmes d'information

APT : Advanced Persistent Threat

BATXH : Baidu, Alibaba, Tencent, Xiaomi, Huaweï

CCI : Chambre de Commerce et d'Industrie

CERT : Computer Emergency Response Team

CETISME : Co-operation to promote Economic and Technological influence in Small and Medium-sized Enterprises

CIA : Central Intelligence Agency

CIHRS : Cairo Institute for Human Rights Studies

CNIL : Commission Nationale de l'Informatique et des Libertés

CSIRT : Computer Security Incident Response Team

DIESE : Diagnostic d'Intelligence Économique et de Sécurité des Entreprises

D2IE : Délégation interministérielle à l'intelligence économique

DGSI : Direction générale de la sécurité intérieure

DRSD : Direction du Renseignement et de la Sécurité de la Défense

ETI : Entreprise de taille intermédiaire

EUIPO : Office de l'Union Européenne pour la Propriété Intellectuelle

FBI : Federal Bureau of Investigation

FIDH : Fédération internationale pour les droits humains

FOVI : Faux Ordres de Virement

GAFAM : Google, Apple, Facebook, Amazon, Microsoft

GI : Guerre de l'information

ICP : Indicateur clé de performance (KPI en Français)

IE : Intelligence économique

INPI : Institut National de la Propriété Industrielle

IT : Information Technology

KPI : Key Performance Indicator (ICP en Français)

LPM : Loi de programmation militaire

MFA : Multi-factor authentification

NIC : National Intelligence Council

NTIC : Nouvelles technologies de l'information et de la communication

OBSARM : Observatoire des Armements

OSINT : Open source intelligence (ROSO en Français)

PME : Petite ou moyenne entreprise

PMI : Petite ou moyenne industrie

ROSO : Renseignement d'origine sources ouvertes (OSINT en Anglais)

RGPD : Règlement Général sur la Protection de Données

SCIE : Service de coordination à l'intelligence économique

SGDSN : Secrétariat général de la défense et de la sécurité nationale

SISSE : Service de l'information stratégique et de la sécurité économique

SYNFIE : Syndicat français de l'intelligence économique

TTP : Tactics Technics & Procédures

7.5. Bibliographie

Les références bibliographies, disponibles en bas de page, sont listée ci-dessous par ordre d'apparition dans le document.

BALIMA Serge Théophile. « Une ou des « sociétés de l'information » ? », *Hermès, La Revue*, 2004/3 (n° 40), p. 205-209. DOI : 10.4267/2042/9540. URL : **https://www.cairn.info/revue-hermes-la-revue-2004-3-page-205.htm** ; consulté le 21/04/2022

MARTRE, Henri. 1994. *Intelligence économique et stratégie des entreprises.* Paris : La Documentation Française. Premier rapport étatique comportant le terme intelligence économique dans son titre. Page 11

Centre de ressources et d'information sur l'intelligence économique et stratégique. Guerre de l'information. *Portail de l'IE.* [En ligne] [Consulté le : 25 mars 2022.] https://portail-ie.fr/resource/glossary/97/guerre-de-linformation.

HARBULOT, Christian. 2001. Les principes de la guerre de l'information. *Infoguerre.* [En ligne] 14 novembre 2001. [Consulté le 25 mars 2022.] https://www.ege.fr/infoguerre/2001/11/les-principes-de-la-guerre-de-l-information.

Olivier de Maison Rouge, Le droit du renseignement. Renseignement d'État; Renseignement économique, LexisNexis, 2016

État-major des armées. 2021. Vision stratégique du Chef d'État-major des armées. [En ligne] octobre 2021. [Consulté le 25 mars 2022.] https://www.defense.gouv.fr/sites/default/files/ema/211022_EMACOM_VisionStrategiqueCEMA_FR_Vdef_HQ%20%282%29.pdf.

LAÏDI Ali, Une histoire de la guerre économique in Christian Harbulot, Manuel d'Intelligence économique. 3ème édition, 2019, PUF, 43-54

IAE Lille - Ecole Universitaire de Management. 2012. La stratégie d'entreprise selon Michael Porter. [En ligne] 10 mars 2012. [Consulté le 26 avril 2022.] https://modules-iae.univ-lille.fr/M03/cours/co/ch1_01.html.

Ministère de l'Intérieur. 2021. Ingérence économique - De l'importance de contrôler l'honorabilité et la réputation de ses partenaires commerciaux. [En ligne] mai 2021. [Consulté le 25 mars 2022.] Flash DGSI #74. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Contr%C3%B4le%20de%20l%27honorabilit%C3%A9%20et%20de%20la%20r%C3%A9putation%20de%20ses%20partenaires%20commerciaux-Mai%202021.pdf.

Ministère de l'Intérieur. 2020. Ingérence économique - Les risques liés à l'hébergement de données dans le Cloud. [En ligne] novembre 2020. [Consulté le 25 mars 2022.] Flash DGSI #69. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Risques%20li%C3%A9s%20%C3%A0%20l%27usage%20du%20Cloud%20Novembre%202020_0.pdf.

Ministère de l'Intérieur. 2020. Ingérence économique - Les risques de captation d'informations liés aux partenariats déséquilibrés avec des acteurs étrangers. [En ligne] décembre 2020. [Consulté le 25 mars 2022.] Flash DGSI #70. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Les%20risques%20li%C3%A9s%20aux%20partenariats%20d%C3%A9s%C3%A9quilibr%C3%A9s%20avec%20des%20acteurs%20%C3%A9trangers%20d%C3%A9loyaux%20d%C3%A9cembre%202020.pdf.

[1]**Ministère de l'Intérieur. 2021.** Ingérence économique - Questionnaires et entretiens rémunérés. [En ligne] décembre 2021. [Consulté le 26 mars 2022.] Flash DGSI #79. https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-12/Questionnaires%20et%20entretiens%20r%C3%A9mun%C3%A9r%C3%A9s-%20d%C3%A9cembre%202021.pdf.

Ministère de l'Intérieur. 2021. Ingérence économique - Le dénigrement commercial, facteur de pertes de marchés et déstabilisation financière. [En ligne] juin 2021. [Consulté le 26 mars 2022.] https://www.dgsi.interieur.gouv.fr/sites/dgsi/files/2021-06/Ing%C3%A9rence%20d%C3%A9nigrement%20commercial-Juin%202021.pdf.

VILLARS, Nathalie. 2021. Artisans, PME, médecins… quand les rumeurs ruinent nos entrepreneurs. *Capital.* [En ligne] 19 avril 2021. [Consulté le 26 mars 2022.] https://www.capital.fr/votre-carriere/artisans-pme-medecins-quand-les-rumeurs-ruinent-nos-entrepreneurs-1400414.

Code pénal, article 323-1, version en vigueur depuis le 27 juillet 2015, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939438/, consulté le 17 avril 2022

Code pénal, article 323-2, version en vigueur depuis le 27 juillet 2015, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939443, consulté le 17 avril 2022

Code pénal, article 323-3, version en vigueur depuis le 27 juillet 2015, modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939448, (consulté le 17 avril 2022)

Code pénal, article 323-3-1, version en vigueur depuis le 20 décembre 2013, modifié par LOI n°2013-1168 du 18 décembre 2013 - art. 25, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345220, consulté le 17 avril 2022

Code pénal, article 323-6, version en vigueur depuis le 14 mai 2009, modifié par LOI n°2009-526 du 12 mai 2009 - art. 124, [En ligne] lien : https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020630782, consulté le 17 avril 2022

Code de la propriété intellectuelle, article L342-1, version en vigueur depuis le 01 janvier 1998, création Loi n°98-536 du 1 juillet 1998 - art. 5 () JORF 2 juillet 1998 en vigueur le 1er janvier 1998, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006279247, consulté le 17 avril 2022

Code de la propriété intellectuelle, article L342-2, version en vigueur depuis le 01 janvier 1998, Création Loi n°98-536 du 1 juillet 1998 - art. 5 () JORF 2 juillet 1998 en vigueur le 1er janvier 1998, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006279250/, consulté le 17 avril 2022

BARBRY Eric. 2020. Risques légaux pour la veille / investigation en ligne ? - Club OSINT & Veille AEGE / Cabinet Racine, Conférence TVAEGE [en ligne], 25 octobre 2020 [consulté le 17 avril 2022], disponible à l'adresse : https://www.youtube.com/watch?v=to6c7wGXhAc,

CNIL. 2021. RGPD : de quoi parle-t-on ? [En ligne] 2021. [Consulté le 15 avril 2022.] https://www.cnil.fr/fr/rgpd-de-quoi-parle-t-on .

CNIL. 2022. Fuite de données de santé : sanction de 1,5 million d'euros à l'encontre de la société DEDALUS BIOLOGIE. [En ligne] 21 avril 2022. [Consulté le 05 mai 2022.] https://www.cnil.fr/fr/fuite-de-donnees-de-sante-sanction-de-15-million-deuros-lencontre-de-la-societe-dedalus-biologie .

Code pénal, article 226-18, version en vigueur depuis le 07 août 2004, modifié par Loi n°2004-801 du 6 août 2004 - art. 14 () JORF 7 août 2004, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000006417968/, [consulté le 17 avril 2022]

DE MAISON ROUGE Olivier. Note - Guide d'application du Règlement européen (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel. Support de cours Ecole de Guerre Economique. 2022, p.32

Légifrance. 2018. LOI n° 2018-670 du 30 juillet 2018 relative à la protection du secret des affaires. [En ligne] 30 juillet 2018. [Consulté le 02 mai 2022.] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000037262111 .

CCI Ile-de-France. 2020. Secret des affaires - Comment bénéficier de la protection prévue par la loi du 30 juillet 2018 ? [En ligne] 04 décembre 2020. [Consulté le : 02 mai 2022.] https://www.cci-paris-idf.fr/sites/default/files/2020-12/guide-secret_des_affaires.pdf.

Code de commerce, article L151-1, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266553/, consulté le 17 avril 2022

code de commerce, article L151-2, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266557 , consulté le 17 avril 2022

Code de commerce, article L151-4, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037266563 , consulté le 17 avril 2022

Code de commerce, article L151-5, version en vigueur depuis le 01 août 2018, création LOI n° 2018-670 du 30 juillet 2018 - art. 1, . [En ligne] https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000037266565/2021-07-13, consulté le 17 avril 2022

HAAS, Gérard et CADOT, Marie . 2021. Dénigrement et pratique commerciale trompeuse : Yuka condamnée. *HAAS Avocats*. [En ligne] 2021. [Consulté le 05 mai 2022.] https://info.haas-avocats.com/droit-digital/denigrement-et-pratique-commerciale-trompeuse-yuka-condamnee.

Avocats Picovschi. 2021. Concurrence déloyale et parasitisme. *Avocats-Picovschi*. [En ligne] 29 septembre 2021. [Consulté le 13 mars 2022.] https://www.avocats-picovschi.com/concurrence-deloyale-et-parasitisme_menu2_67_14.html.

Vie Publique. 2022. Loi du 21 mars 2022 visant à améliorer la protection des lanceurs d'alerte. [En ligne] 22 mars 2022. [Consulté le 01 avril 2022.] https://www.vie-publique.fr/loi/282472-loi-21-mars-2022-waserman-protection-des-lanceurs-dalerte .

LOI n° 2016-1691 relative à la transparence, à la lutte contre la corruption et à la modernisation de la vie économique (1), [En ligne] 9 décembre 2016, [consulté le 24 avril 2022] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528/

Le Mag IT. 2018. Quelles différences entre CLOUD Act et PATRIOT Act (et quels impacts sur les entreprises françaises). [En ligne] 21 août 2018. [Consulté le 01 avril 2022.] https://www.lemagit.fr/conseil/Quelles-differences-entre-CLOUD-Act-et-PARTIOT-Act-et-quels-impacts-sur-les-entreprises-francaises.

BOHIC, Clément. 2022. Scraping : LinkedIn à nouveau freiné dans son combat. *Silicon*. [En ligne] 9 avril 2022. [Consulté le 29 avril 2022.] https://www.silicon.fr/scraping-linkedin-freine-combat-436577.html.

Cabinet Soulier Avocats. 2020. Un post Facebook à ses « amis » peut conduire au licenciement. [En ligne] 30 octobre 2020. [Consulté le 29 avril 2022.] https://www.soulier-avocats.com/un-post-facebook-a-ses-amis-peut-conduire-au-licenciement/.

LEGALIS. 2017. Condamnation pour collecte et extraction frauduleuse de données. [En ligne] 7 novembre 2017. [Consulté le 29 avril 2022.] https://www.legalis.net/actualite/condamnation-pour-collecte-et-extraction-frauduleuse-de-donnees/.

Zscaler. 2021. What Is Double Extortion Ransomware? [En ligne] 2021. [Consulté le 05 mai 2022.] https://www.zscaler.com/resources/security-terms-glossary/what-is-double-extortion-ransomware.

DECHY Anthony et CAPILLIEZ Cyril. Tour d'horizon du *framework* MITRE ATT&CK. Blog Advens. 2022 [Consulté le 02 mai 2022]. Disponible à l'adresse : https://www.advens.fr/fr/ressources/blog/tour-dhorizon-du-framework-mitre-attck

The MITRE Corporation. *Versions of ATT&CK*. MITRE ATT&CK [en ligne]. 2022. [Consulté le 02 mai 2022]. Disponible à l'adresse : https://attack.mitre.org/resources/versions/

The MITRE Corporation. *Enterprise Matrix*. MITRE ATT&CK [en ligne]. 2022. [Consulté le 02 mai 2022]. Disponible à l'adresse : https://attack.mitre.org/matrices/enterprise/

The MITRE Corporation. *Updates – April 2022*. MITRE ATT&CK [en ligne]. 2022. [Consulté le 02 mai 2022]. Disponible à l'adresse : https://attack.mitre.org/resources/updates/updates-april-2022/

BERGERON, Pierette , et al. 2009. *La gestion stratégique de l'information dans Introduction aux sciences de l'information*. Montréal : Presses de l'Université de Montréal, 2009. p. 235. ISBN : 978-2-7606-2114-5.

CARAYON, Bernard. 2003. Intelligence économique, compétitivité et cohésion sociale. Paris : s.n., 2003.

Rapport Digimind. 2017. Les 20 bonnes pratiques essentielles pour votre projet de veille. 2017.

NANECHE, Matmar. 2018. La veille stratégique au sein des entreprises modernes. [En ligne] 2018. [Consulté le 17 avril 2022.] https://atlas.irit.fr/PIE/VSST/Actes-VSST2018-Toulouse/Matmar-Naneche.pdf.

CHAABEN, Mariem et FOUGHALI, Wafa. 2017. La cellule de veille au sein du CTAA (Centre Technique de l'agro-alimentaire). [En ligne] 23 mars 2017. [Consulté le 27 avril 2022.] https://fr.slideshare.net/mariemchaaben/etude-decascelluledeveille.

BENOIT-CERVANTES, Géraldine. 2017. La veille sur Internet. [En ligne] 30 novembre 2017. [Consulté le 27 avril 2022.] https://www.e-marketing.fr/Thematique/academie-1078/fiche-outils-10154/La-veille-sur-Internet-324957.htm#.

GLOAGUEN, Philippe. Le guide l'intelligence économique. Le Routard. [en ligne]. 1° édition. Italie : HACHETTE LIVRE 2014. 143 pages. ISBN-301-00-00-03-62-96 [consulté le 12 mai 2022]. Disponible à l'adresse : https://www.entreprises.gouv.fr/files/files/directions_services/information-strategique-sisse/routard-guide-intelligence-economique.pdf

BELIMANE, Wissam et RHANI, Amel. 2010. La mise en place d'un système de veille commerciale. [En ligne] 2010. [Consulté le 26 avril 2022.] https://www.memoireonline.com/12/11/4977/m_La-mise-en-place-dun-systeme-de-veille-commerciale5.html.

GEROUDET, Marie-Madeleine. 2013. Types de veilles. [En ligne] 2013. [Consulté le 28 avril 2022.] http://www.ressources.univ-rennes2.fr/cultures-numeriques-dans-l-enseignement/veille/1-quest-ce-que-la-veille/types-de-veilles/.

Université de Rennes 2. Définitions de la veille. [En ligne] [Consulté le 28 avril 2022.] http://www.ressources.univ-rennes2.fr/cultures-numeriques-dans-l-enseignement/veille/1-quest-ce-que-la-veille/1-1-definitions-de-la-veille/.

GUECHTOULI, Manelle et BOUDRANDI, Stéphane. 2013. Comment se « fabrique » la décision stratégique : le cas d'une cellule de veille stratégique. *CAIRN.INFO*. [En ligne] 01 novembre 2013. [Consulté le 27 avril 2022.] https://www.cairn.info/revue-recherches-en-sciences-de-gestion-2012-1-page-35.htm.
MARQUANT, Arnaud. 2022. Mise en place d'une cellule de veille au sein de l'entreprise : trois actions à consolider. *Global Security Mag*. [En ligne] février 2022. [Consulté le 29 avril 2022.] https://www.globalsecuritymag.fr/Mise-en-place-d-une-cellule-de,20220222,122305.html.

Vegenov. 2017. Externaliser sa veille : une solution aux multiples avantages. *Vegenov*. [En ligne] juin 2017. [Consulté le 29 avril 2022.] https://blog.vegenov.com/2017/06/externaliser-veille-solution-aux-multiples-avantages/.

Inevidence. 2007. *De l'utilité ou de la nécessité d'externaliser toute ou partie de la veille.* [Présentation Powerpoint] Rabat : s.n., 24 et 25 mai 2007. Séminaire « Veille et Text-Mining ».

Digimind et Orange Consulting. 2021. *État de l'art & Tendance Veille et Market Intelligence.* 2021.

TROUCHAUD, Philippe. 2016. *La cybersécurité au-delà de la technologie*. Paris : Odile Jacob, 2016. pp. 42-43. IBSN : 978-2-7381-3368-7.

GARO, Jean-Denis. 2021. Le paradoxe de la charge des données. *La Tribune*. [En ligne] 08 septembre 2021. [Consulté le 25 avril 2022.] https://www.latribune.fr/opinions/tribunes/le-paradoxe-de-la-charge-des-donnees-891771.html.

Forrester. mai 2021. *Businesses Must Better Balance Culture And Technology To Improve Data Readiness*. mai 2021. Étude commandée par Dell Technologies.

MongoDB. 2021. Unstructured Data. *MongoDB*. [En ligne] 2021. [Consulté le 28 avril 2022.] https://www.mongodb.com/unstructured-data.

Converteo. 2017. 10 critères RGPD pour évaluer vos bases de données. *Converteo*. [En ligne] 11 octobre 2017. [Consulté le 28 avril 2022.] https://converteo.com/blog/10-criteres-rgpd-pour-evaluer-vos-bases-de-donnees/.

LUSSAN, Pierre-Louis. 2022. Comment élaborer une politique efficace de classification des données pour une meilleure sécurité de l'information. Netwrix. [En ligne] 13 janvier 2022. [Consulté le 2022 avril 30.] https://blog.netwrix.fr/2018/06/20/comment-elaborer-une-politique-efficace-de-classification-des-donnees-pour-une-meilleure-securite-de-linformation/.

TROUCHAUD, Philippe. 2016. *La cybersécurité au-delà de la technologie*. Paris : Odile Jacob, 2016. pp. 42-43. ISBN : 978-2-7381-3368-7

CNRS. 2014. Le cycle de vie des données. *inist*. [En ligne] Institut de l'Information Scientifique et Technique, 16 septembre 2014. [Consulté le 30 avril 2022.] https://www.inist.fr/wp-content/uploads/donnees/co/module_Donnees_recherche_7.html#:~:text=D%C3%A9finition,des%20donn%C3%A9es%20de%20la%20recherche..

COLLINS, Robert. 2021. Insider Risk Caused By Data Exposure and Leaks Siphons Vast Revenue from Organizations. *BusinessWire*. [En ligne] 07 juillet 2021. [Consulté le 14 avril 2022.] https://www.businesswire.com/news/home/20210707005267/en/Insider-Risk-Caused-By-Data-Exposure-and-Leaks-Siphons-Vast-Revenue-from-Organizations.

Aberdeen Group. Juin 2021. *Understanding Your Insider Risk and the Value of Your IP*. Juin 2021.

Ponemon Institute & Proofpoint. 2022. *2022 costs of insider threats global report*. 2022.

MEDDAH, Hassan. 2019. Les sous-traitants, le nouveau maillon faible de la chaîne de la cybersécurité. *L'usine Nouvelle*. [En ligne] 23 janvier 2019. [Consulté le 02 mai 2022.] https://www.usinenouvelle.com/article/les-sous-traitants-le-nouveau-maillon-faible-de-la-chaine-de-la-cybersecurite.N796835.

S., Elina. 2020. SolarWinds : tout savoir sur la cyberattaque historique des États-Unis. *Le Big Data*. [En ligne] 22 décembre 2020. [Consulté le 02 mai 2022.] https://www.lebigdata.fr/solarwinds-cyberattaque-historique-usa.

BlueVoyant. 2021. *Managing Cyber Risk Across the Extended Vendor Ecosystem*. New York City : BlueVoyant, 2021.

JONES, Isa. 2022. 'Hack One, Breach Many' Is Here to Stay: How to Secure Your Third-Party Risks. *Infosecurity*. [En ligne] 26 janvier 2022. [Consulté le 02 mai 2022.] https://www.infosecurity-magazine.com/blogs/how-to-secure-your-thirdparty-risks/.

SecureLink & Ponemon Institute. 2021. *A crisis in third-party remote access security*. 2021.

HackerOne. 2021. *The Corporate Security Trap - Shifting security culture from secrecy to transparency*. 2021.

CPR Asset Management. 2021. LA CYBERSÉCURITÉ - NOUVEL ENJEU CLÉ POUR LES ENTREPRISES. *CPR Asset Management*. [En ligne] 08 novembre 2021. [Consulté le 27 février 2022.] https://www.cpr-am.fr/Local-content/Actualites-Presse-Recompenses/La-cybersecurite-Nouvel-enjeu-cle-pour-les-entreprises.

Appitel Beside. 2021. POURQUOI FORMER VOS SALARIÉS À LA SÉCURITÉ INFORMATIQUE ? *Appitel Beside*. [En ligne] 29 mars 2021. [Consulté le 03 mars 2022.] https://www.appitel.fr/blog/appitel/pourquoi-former-vos-salaries-a-la-securite-informatique/.

Tanium Inc. and Nasdaq, Inc. 2016. *THE ACCOUNTABILITY GAP : CYBERSECURITY & BUILDING A CULTURE OF RESPONSIBILITY*. University of London : s.n., 2016.

CyLumena. 2021. Four Areas Where You're Spending Too Much and Four Where You're Spending Too Little on Cybersecurity. *CyLumena*. [En ligne] 2021. [Consulté le 04 mars 2022.] https://www.cylumena.com/insights/reallocate-cyber-budget/.

OLSON, Jason. 2022. Why Cybersecurity Awareness in the Workplace is Everyone's Business. *EideBailly*. [En ligne] 2022. [Consulté le 04 mars 2022.] https://www.eidebailly.com/insights/articles/legacy/cyber-from-the-break-room-to-the-board-room.

Journal Du Net. 2019. E-réputation : définition, synonyme et traduction. *Journal Du Net*. [En ligne] 13 mars 2019. [Consulté le 15 mars 2022.] https://www.journaldunet.fr/business/dictionnaire-du-marketing/1207880-e-reputation-definition-et-traduction/#:~:text=D%C3%A9finition%20du%20mot%20e%2Dreputation,r%C3%A9seaux%20sociaux%2C%20blogs%20ou%20forums..

Qualtrics. 2022. Brand perception: Everything you need to know. *Qualtrics XM*. [En ligne] 2022. [Consulté le 15 mars 2022.] https://www.qualtrics.com/uk/experience-management/brand/brand-perception/?rid=ip&prevsite=fr&newsite=uk&geo=FR&geomatch=uk.

COHEN, Eloïse. 2020. Infographie Que pensent les Français des avis clients? *eMarketing*. [En ligne] 03 janvier 2020. [Consulté le 12 mars 2022.] https://www.e-marketing.fr/Thematique/retail-1095/Infographies/Que-pensent-Fran-ais-avis-clients-345324.htm

Digimind. 2022. L'impact déterminant de la réputation en phase d'achat : l'histoire du VTT d'Arthur. *Digimind*. [En ligne] 18 février 2022. [Consulté le 12 mars 2022.] https://blog.digimind.com/fr/insight-driven-marketing/impact-determinant-de-reputation-en-phase-dachat.

Semji. 2022. Comment maîtriser son e-réputation ? *Semji*. [En ligne] 2022. [Consulté le 12 mars 2022.] https://semji.com/fr/guide/e-reputation/.

Opinion Act. 2019. Parts de marché des moteurs de recherche dans le monde. *Opinion Act*. [En ligne] 2019. [Consulté le 12 mars 2022.] https://www.opinionact.com/ressources/seo-content-marketing/parts-de-marche-des-moteurs-de-recherche-dans-le-monde.

Les Echos Entrepreneurs. 2014 . Zones de description et notoriété des pages. *Les Echos*. [En ligne] 14 mai 2014 . [Consulté le 12 mars 2022.] https://business.lesechos.fr/entrepreneurs/web/dossiers/4174762/tpepme-0004174762-2-zones-de-description-et-notoriete-des-pages-63781.php.

ASSELIN, Christophe. 2021. Les réseaux sociaux en France et dans le monde : les chiffres d'utilisation en 2021. *Digimind*. [En ligne] 21 avril 2021. [Consulté le 12 mars 2022.] https://blog.digimind.com/fr/tendances/r%C3%A9seaux-sociaux-france-monde-chiffres-utilisation-2021.

Net Offensive. 2018. Influenceurs et e-réputation de l'entreprise et marque en ligne. *Net Offensive*. [En ligne] 2018. [Consulté le 12 mars 2022.] https://www.netoffensive.blog/e-reputation/ameliorer/influenceurs/.

SALGUES, Floriane. 2017. Quel est l'impact des influenceurs sur les consommateurs ? *eMarketing*. [En ligne] 18 octobre 2017. [Consulté le 12 mars 2022.] https://www.e-marketing.fr/Thematique/social-media-1096/Infographies/Quel-est-impact-influenceurs-consommateurs-322071.htm#.

SIX, Nicolas. 2022. Cinq étoiles et 10/10 : pourquoi il ne faut pas faire confiance aux notes des internautes. *Le Monde*. [En ligne] 19 janvier 2022. [Consulté le 12 mars 2022.] https://www.lemonde.fr/pixels/article/2022/01/19/cinq-etoiles-et-10-10-pourquoi-il-ne-faut-pas-faire-confiance-aux-notes-des-internautes_6110162_4408996.html.

Semji. 2014. Bad buzz intentionnel : quand les marques surfent sur le buzz négatif. [En ligne] 2014. [Consulté le 12 mars 2022.] https://semji.com/fr/blog/bad-buzz-intentionnel-quand-les-marques-surfent-sur-le-buzz-negatif.

MOINET, Nicolas. 2020. Les sentiers de la Guerre Economique 2 «Soft Powers». Versailles : VA Editions Collection «Indiscipliné», 2020. p. 100. ISBN 978-2-36093-117-0.

La Tribune. 2001. *Un seul homme peut déstabiliser une multinationale*. 11 avril 2001. Propos de Christian Harbulot recueillis par Sandrine L'Herminier.

Ministère de la Culture. 2018. FAKE NEWS. *Ministère de la Culture*. [En ligne] 4 octobre 2018. [Consulté le 12 mars 2022.] http://www.culture.fr/Ressources/FranceTerme/Recommandations-d-usage/FAKE-NEWS.

CHAIEHLOUDJ, Walid. 2018. Fake news et droit de la concurrence : réflexions au prisme des cas Facebook et Google. *Cairn.info*. [En ligne] Revue internationale de droit économique , 09 juillet 2018. [Consulté le 12 mars 2022.] https://www.cairn.info/revue-internationale-de-droit-economique-2018-1-page-17.htm?contenu=auteurs.

SILINI, Alberto. 2019. Cinquante nuances de désinformation. *EJO*. [En ligne] 28 novembre 2019. [Consulté le 14 mars 2022.] https://fr.ejo.ch/deontologie-qualite/cinquante-nuances-desinformation-fakenews-trouble-information-claire-wardle-manipulation.

GHERARDI, Alexandra. 2014. Le dénigrement commercial et la diffamation, une subtile différence. *avocats-picovschi*. [En ligne] 20 octobre 2014. [Consulté le 12 mars 2022.] https://www.avocats-picovschi.com/le-denigrement-commercial-et-la-diffamation-une-subtile-difference_article_948.html.

MARTIN, Isabelle. 2021. FAKE NEWS, INFOX, DE QUOI PARLE-T-ON ? *Clemi*. [En ligne] 2021. [Consulté le 12 mars 2022.] https://www.clemi.fr/fr/evenements/operations-speciales/exposition-fake-news-art-fiction-mensonge/la-fabrication-des-fake-news/fake-news-infox-de-quoi-parle-t-on.html.

BRONNER, Gérald. Janvier 2022. *Les Lumières à l'ère numérique*. Paris : Rapport de la Commission, Janvier 2022.

CATHARING. 2020. L'encerclement cognitif, mode d'emploi. *Olduvaï*. [En ligne] 10 février 2020. [Consulté le 02 mai 2022.] https://www.le-projet-olduvai.com/t11696-l-encerclement-cognitifmode-d-emploi.

FÉDÉRATION INTERNATIONALE POUR LES DROITS HUMAINS. 2018. Egypte : une répression made in France. *FIDH*. [En ligne] 02 juillet 2018. [Consulté le : 26 avril 2022.] https://www.fidh.org/fr/regions/maghreb-moyen-orient/egypte/egypte-une-repression-made-in-france.

Ecole de Guerre Economique (MSIE36). 2021. Comment les États-Unis contribuent-ils à affaiblir l'économie française ? *EGE*. [En ligne] v12.1, Octobre 2021. [Consulté le 02 mai 2022.] MSIE36 sous la direction de Christian HARBULOT. https://www.ege.fr/sites/ege.fr/files/media_files/rapport_alerte_usa_2021.pdf.

FERRIA, Haroun et VACHEL, Julien. 2019. Les think tanks français : des lobbies intellectualisés ? *portail-ie*. [En ligne] 11 février 2019. [Consulté le 02 mai 2022.] https://portail-ie.fr/analysis/2061/les-think-tanks-francais-des-lobbies-intellectualises.

ASTIER, Stéphane et POUJOL, Axelle . 2019. Cybersécurité : comment lutter contre les opérations de déstabilisation et d'influence ? *info.haas-avocats*. [En ligne] 2019. [Consulté le 03 mai 2022.] https://info.haas-avocats.com/droit-digital/cybersecurite-comment-lutter-contre-les-operations-de-destabilisation-et-d-influence.

KINSTA. 2020. Que sont les DNS ? Explication du système de noms de domaine. *KINSTA*. [En ligne] 6 janvier 2020. [Consulté le 20 mars 2022.] https://kinsta.com/fr/base-de-connaissances/que-sont-les-dns/.

[1] **Avocats Picovschi . 2016.** Mon concurrent a réservé mon nom de domaine : quels sont mes recours ? *Avocats-Picovschi* . [En ligne] 23 mars 2016. [Consulté le 20 mars 2022.] https://www.avocats-picovschi.com/mon-concurrent-a-reserve-mon-nom-de-domaine-quels-sont-mes-recours_article_1159.html.

INLEX IP EXPERTISE. 2015. Quand Google perd son nom de domaine « google.com. *INLEX IP EXPERTISE*. [En ligne] 19 octobre 2015. [Consulté le 20 mars 2022.] https://ip-talk.com/2015/10/19/quand-google-perd-son-nom-de-domaine-google-com/.

Journal Du Net. 2021. Cybersquatting : définition, exemples et textes de loi. *Journal Du Net*. [En ligne] 21 décembre 2021. [Consulté le 20 mars 2022.] https://www.journaldunet.fr/business/dictionnaire-du-droit-des-affaires/1507643-cybersquatting-definition-exemples-et-textes-de-loi/.

AUTISSIER, Charlotte. 2021. Nom de domaine : pourquoi et comment l'enregistrer ? Legalstart. [En ligne] 26 mai 2021. [Consulté le 20 mars 2022.] https://www.legalstart.fr/fiches-pratiques/astuces-entrepreneurs/nom-de-domaine/#:~:text=La%20d%C3%A9finition%20d'un%20nom,acc%C3%A9der%20%C3%A0%20un%20site%20internet.

Menlo Security. 2018. HOW CYBERCRIMINALS ARE EXPLOITING TRADITIONAL MEASURES OF TRUST. [En ligne] 5 février 2018. [Consulté le 20 mars 2022.] https://info.menlosecurity.com/rs/281-OWV-899/images/Menlo_TrustHacking_Infographic_Final.pdf.

RIEß-MARCHIVE, Valéry. 2016. Vinci victime d'une arnaque bien organisée. *Le Mag IT*. [En ligne] 23 novembre 2016. [Consulté le 21 mars 2022.] https://www.lemagit.fr/actualites/450403436/Vinci-victime-dune-arnaque-bien-organisee.

WEISE, Elizabeth. 2016. Hackers use typosquatting to dupe the unwary with fake news, sites. *USA Today Tech*. [En ligne] 01 décembre 2016. [Consulté le 20 mars 2022.] https://eu.usatoday.com/story/tech/news/2016/12/01/hackers-use-typo-squatting-lure-unwary-url-hijacking/94683460/.

AFNIC. 2018. Cybersquatting, Spam, Phishing... les différents types d'abus sur noms de domaine. [En ligne] 06 septembre 2018. [Consulté le 20 mars 2022.] https://www.afnic.fr/observatoire-ressources/papier-expert/cybersquatting-spam-phishing-les-differents-types-dabus-sur-noms-de-domaine/.

BANCAL, Damien. 2018. Fraude aux couleurs d'Air France. *Zataz*. [En ligne] 13 février 2018. [Consulté le 21 mars 2022.] https://www.zataz.com/fraude-aux-couleurs-dair-france/.

Barracuda. 2020. 13 types d'attaques par e-mail à connaître immédiatement. *Barracuda*. [En ligne] Mai 2020. [Consulté le 22 mars 2022.] https://assets.barracuda.com/assets/docs/dms/eBook_email-threats_fr-FR.pdf.

Barracuda. 2022. Malware. [En ligne] 2022. [Consulté le 21 mars 2022.] https://fr.barracuda.com/glossary/malware#section_3.

CAPRONI, Nicolas. 2013. Un CSIRT, à quoi ça CERT ? *CYBER-SECURITE*. [En ligne] 13 décembre 2013. [Consulté le 15 avril 2022.] https://www.cyber-securite.fr/2013/12/13/un-csirt-a-quoi-ca-cert/.

CERT-FR. 2022. INTERCERT FRANCE. *CERT-FR*. [En ligne] 2022. [Consulté le 15 avril 2022.] https://www.cert.ssi.gouv.fr/csirt/intercert-fr/.

InCyber. 2022. France : l'ANSSI créé sept CSIRT régionaux. *inCyber*. [En ligne] 12 janvier 2022. [Consulté le : 29 avril 2022.] https://incyber.org/france-anssi-cree-sept-csirt-regionaux/.

PwC France. 2021. Espionnage industriel - Une menace à appréhender avec détermination. [En ligne] 2021. [Consulté le 19 avril 2022.] https://www.pwc.fr/fr/decryptages/securite/espionnage-industriel-menace-a-apprehender-avec-determination.html.

ANSSI. Une attaque réussie : combien de marchés potentiels perdus ? *ssi.gouv*. [En ligne] [Consulté le : 19 avril 2022.] https://www.ssi.gouv.fr/entreprise/principales-menaces/espionnage/.

Ouest-France. 2018. Comment les Russes ont espionné l'équipe Clinton, et chamboulé la présidentielle américaine. *Ouest-France*. [En ligne] 13 juillet 2018. [Consulté le : 19 avril 2022.] https://www.ouest-france.fr/monde/états-unis/comment-les-russes-ont-espionne-l-equipe-clinton-et-chamboule-la-presidentielle-americaine-5879669.

BEKY, Ariane. 2021. Sécurité : 175 jours pour détecter une cyberattaque en Europe. *Silicon*. [En ligne] 2 mars 2021. [Consulté le : 20 avril 2022.] https://www.silicon.fr/securite-175-jours-detecter-cyberattaque-europe-205461.html#.

CHANDEZE, Aurélie. 2020. Entre 3 et 7 semaines pour se rétablir après une cyberattaque. *CIO*. [En ligne] 12 novembre 2020. [Consulté le : 19 avril 2022.] https://www.cio-online.com/actualites/lire-entre-3-et-7-semaines-pour-se-retablir-apres-une-cyberattaque-12683.html.

TUNG, Liam. 2021. Voici pendant combien de temps les attaquants se dissimulent dans votre réseau avant de déployer un ransomware ou d'être repérés. *ZDNet*. [En ligne] 20 mai 2021. [Consulté le : 20 avril 2022.] https://www.zdnet.fr/actualites/voici-pendant-combien-de-temps-les-hackers-se-dissimulent-dans-votre-reseau-avant-de-deployer-un-ransomware-ou-d-etre-reperes-39923061.htm.

C-Risk. 2021. What is a MITM attack and how can you protect yourself against it? [En ligne] 10 septembre 2021. [Consulté le : 28 avril 2022.] https://www.c-risk.com/en/blog/mitm-attack/.

IONOS. 2019. Attaque Man in the Middle (MITM). [En ligne] 19 mars 2019. [Consulté le : 28 avril 2022.] https://www.ionos.fr/digitalguide/serveur/securite/attaque-de-lhomme-du-milieu-apercu-du-modele/.

Blackbird. 2020. Black Wifi : l'exemple d'un faux point d'accès. *Les dossiers du Pirate*. SARL ID Presse, octobre - décembre 2020, N°25, pp. 52-53.

Oracle. 2020. Qu'est-ce qu'un sniffer ? *Oracle*. [En ligne] 2020. [Consulté le : 28 avril 2022.] https://www.oracle.com/fr/security/definition-sniffer-renifleur.html.

Département TI. 2020 . Les aspects de sécurité d'un centre de données. *Département TI*. [En ligne] 2020 . [Consulté le : 28 avril 2022.] https://www.departement-ti.com/2019/11/18/les-aspects-de-securite-dun-centre-de-donnees/.

Openpath. 2020. Guide to Physical Security in the Workplace. *Openpath*. [En ligne] 2020. [Consulté le : 09 mai 2022.] https://info.openpath.com/hubfs/Openpath-Physical-Security-Guide.pdf?utm_medium=email&_hsmi=97869752&_hsenc=p2ANqtz-9HZkUjNFJozp3gnkh2XUCbpNGsgxpMqPwky28wFzkdy3xhO28VNgiecOluEbb-qibjwc-9GBMgVxuRUo5c468cPq_EtQ&utm_content=97869752&utm_source=hs_automation.

MORTON, Jennie. 2011. 10 strategies prevent tailgating. *Buildings*. [En ligne] 06 décembre 2011. [Consulté le : 08 mai 2022.] https://www.buildings.com/articles/31764/10-strategies-prevent-tailgating.

IONOS. 2020. Shoulder surfing – un danger sous-estimé ? *IONOS*. [En ligne] 14 septembre 2020. [Consulté le : 08 mai 2022.] https://www.ionos.fr/digitalguide/serveur/securite/shoulder-surfing/#:~:text=Le%20shoulder%20surfing%20fait%20partie,donn%C3%A9es%20par%20une%20observation%20directe.

IFACI et AMRAE. 2013. Trois lignes de maîtrise pour une meilleure performance. *IFACI*. [En ligne] 2013. [Consulté le : 06 mai 2022.] https://docs.ifaci.com/wp-content/uploads/2018/03/Trois_lignes_de_ma%C3%AEtrise_pour_une_meilleure_performance.pdf.

IFACI. 2013. LES MÉTIERS DE L'AUDIT ET DU CONTRÔLE INTERNES. *IFACI*. [En ligne] 2013. [Consulté le : 06 mai 2022.] https://www.ifaci.com/audit-controle-interne/metiers-de-laudit-controle-internes/#:~:text=Le%20contr%C3%B4le%20interne%20est%20un,reporting%20et%20%C3%A0%20la%20conformit%C3%A9..

CYBERARK. 2019. Fuite de données. [En ligne] 2019. [Consulté le : 04 mai 2022.] https://www.cyberark.com/fr/what-is/data-breach/.

NAGEOTTE, Agathe. 2021. Données sensibles des entreprises : comment les sécuriser ? *oodrive*. [En ligne] 19 avril 2021. [Consulté le : 04 mai 2022.] https://www.oodrive.com/fr/blog/securite/donnees-sensibles-entreprise/#:~:text=Pour%20se%20prot%C3%A9ger%2C%20il%20est,confidentialit%C3%A9%20des%20%C3%A9changes%20est%20essentielle..

Security, IBM. juillet 2021. *Cost of a data breach report*. New York : s.n., juillet 2021.

Rapid7. 2019. What is user and entity behavior analytics? (UEBA). *Rapid7*. [En ligne] 2019. [Consulté le : 27 avril 2022.] https://www.rapid7.com/fundamentals/user-behavior-analytics/.

Proofpoint. 2021. Qu'est-ce que la Data Loss Prevention (DLP) ? *proofpoint*. [En ligne] 2021. [Consulté le : 23 mai 2022.] https://www.proofpoint.com/fr/threat-reference/dlp.

LAMIGEON, Vincent. 2021. CybelAngel, la pépite cyber française, entre au Next40. *Challenges*. [En ligne] 08 février 2021. [Consulté le 03 mai 2022.] https://www.challenges.fr/entreprise/cybelangel-la-pepite-cyber-francaise-entre-au-next40_750002.

KLEN, Michel. 2020. La désinformation opérationnelle. *Cairn.info*. [En ligne] 17 février 2020. [Consulté le : 15 avril 2022.] cairn.info/revue-defense-nationale-2016-1-page-114.htm?contenu=resume.

L'internaute. 2021. Obfuscation. *l'internaute*. [En ligne] 01 janvier 2021. [Consulté le : 13 mai 2022.] https://www.linternaute.fr/dictionnaire/fr/definition/obfuscation/#:~:text=L'obfuscation%20consiste%20%C3%A0%20prot%C3%A9ger,suppression%20de%20donn%C3%A9es%20trop%20personnelles..

DELAHAYE, Jean-Paul. 2019. L'offuscation ou l'art de brouiller l'écoute. *Pour La Science*. [En ligne] 29 octobre 2019. [Consulté le : 30 mars 2022.] https://www.pourlascience.fr/sr/logique-calcul/l-offuscation-ou-l-art-de-brouiller-l-ecoute-18265.php.

Talend. 2022. What is Data Obfuscation? *Talend*. [En ligne] 2022. [Consulté le : 28 mars 2022.] https://www.talend.com/resources/data-obfuscation/.

IONOS. 2017. Honeypot - sécurité informatique via des leurres. *IONOS*. [En ligne] 08 août 2017. [Consulté le : 04 mai 2022.] https://www.ionos.fr/digitalguide/serveur/securite/honeypot-securite-informatique-via-des-leurres/.

SCHNEIDER, Bruce. 2001. Secrets et mensonges - Sécurité numérique dans un monde en réseau. [En ligne] 2001. [Consulté le : 07 mai 2022.] http://strategique.free.fr/archives/textes/hacking/archives_hacking_13.htm.

INPI. 2014. Secret(s) ou brevet(s) ? La réponse de Michelin. [En ligne] 2014. [Consulté le : 18 mai 2022.] https://www.inpi.fr/fr/valoriser-vos-actifs/le-magazine-de-la-valorisation/secrets-ou-brevets-la-reponse-de-michelin.

JUILLET Alain, DAGUZAN Jean-François. L'intelligence économique en question(s). Cairn.info/Sécurité globale 2008/4 (N° 6), p. 9-18. [En ligne] 01/10/2013. [Consulté en mai 2022.] DOI : 10.3917/secug.006.0009. URL : https://www.cairn.info/revue-securite-globale-2008-4-page-9.htm

Portail de l'IE. Les définitions de l'intelligence économique. [En ligne] 19 janvier 2013. [Consulté en mai 2022] https://portail-ie.fr/les-definitions-de-lintelligence-economique

SAURY, Raphaëlle. BONDY, Jérôme ou la vision humaine de l'intelligence économique. 2001. [En ligne] 21 décembre 2011. [Consulté en mai 2022] https://portail-ie.fr/short/198/jerome-bondu-ou-la-vision-humaine-de-lintelligence-economique

BONDU, Bondu. Rôle du consultant en intelligence économique. 2022. [En ligne] 22 février 2022. [Consulté en mai 2022.] https://www.inter-ligere.fr/34metaphore-medicale-sur-l-intelligence-economique/

Cahiers de la Guerre Économique, La nouvelle intelligence juridique #6, édition Les influences, 2022

ANSSI. Tensions Internationales : Renforcement de la vigilance cyber. [En ligne] 14 mars 2022 ; 26 février 2022. [Consulté en mai 2022.] https://www.ssi.gouv.fr/actualite/tensions-internationales-renforcement-de-la-vigilance-cyber/

Portail de l'IE. Dissuasion (par l'information). [En ligne] inconnue. [Consulté en mai 2022.] https://portail-ie.fr/resource/glossary/73/dissuasion-par-linformation

JSTOR. Journal article Cooperation Under the Security Dilemma. [En ligne] inconnue. [Consulté en mai 2022.] https://www.jstor.org/stable/2009958

BADEAU, Cyrille. Fusion/Acquisition : pourquoi les entreprises doivent adopter une stratégie commune de cyber-renseignement. 2018 [En ligne] 9 novembre 2018 ; Mis à jour le 2 mars 2021 https://www.silicon.fr/avis-expert/fusion-acquisition-pourquoi-les-entreprises-doivent-adopter-une-strategie-commune-de-cyber-renseignement

Le droit du renseignement, éditions LexisNexis, avril 2016

Renseignement et sécurité, édition Armand Colin, 2019

Christophe Forster. COLLOQUE AAIE-IHEDN « INTELLIGENCE ECONOMIQUE ET ETHIQUE » [En ligne] date inconnue. [Consulté en mai 2022.] https://ie-ihedn.org/wp-content/uploads/2012/01/COLLOQUE-AAIE-IE-ETHIQUE.pdf

SYNFIE. La charte d'éthique. [En ligne] inconnue. Charte adoptée le 15 avril 2014 [Consulté en mai 2022] https://synfie.fr/le-synfie/la-charte-dethique/

C. Anno. Le droit de l'Intelligence Économique. Le petit juriste. 2015. [En ligne] 29 décembre 2015. [Consulté en mai 2022] https://www.lepetitjuriste.fr/droit-de-lintelligence-economique

Le droit du renseignement, éditions LexisNexis, avril 2016

DYLEWSKI, Philippe. ***Le Renseignement Offensif : 300 techniques, outils et astuces pour tout savoir sur tout le monde, dans les entreprises et ailleurs***, édition Agakure, 2022. ISBN : 9791096819287

DUBOIS, Marion. 2021. Cybersécurité : la filière recrute mais peine à former ses élèves. *Ouest France*. [En ligne] 22 septembre 2021. [Consulté le 28 févier 2022.] https://www.ouest-france.fr/economie/cybersecurite-la-filiere-recrute-mais-peine-a-former-ses-eleves-13ac45e4-118a-11ec-aae0-4d1212b14fe9.

GUIRNARCHAUD, Angèle. 2015. Entreprise recherche (jeunes diplômés) hackers désespérément. *Le Monde*. [En ligne] 13 juin 2015. [Consulté le 28 février 2022.] https://www.lemonde.fr/etudes-superieures/article/2015/06/13/entreprise-recherche-jeunes-diplomes-hackers-desesperement_4653663_4468191.html.

KALUSEVIC, Sacha et GOBRON, Gilles. 2021. *Panorama du marché de l'emploi et du recrutement SI. Paris.* : Michael Page & Choose Your Boss, 2021.

TROUCHAUD, Philippe. 2016. *La Cybersécurité au-delà de la technologie*. Paris : Odile Jacob, 2016. p. 47. ISBN : 978-2-7381-3368-7.

GLOAGUEN, Philippe. Le guide l'intelligence économique. Le Routard. [en ligne]. 1° édition. Italie : HACHETTE LIVRE 2014. 143 pages. ISBN-301-00-00-03-62-96 [consulté le 12 mai 2022].

Service de l'Information Stratégique et de la Sécurité Économique (S.I.S.S.E.). La sécurité économique au quotidien [en ligne]. Novembre 2021. 95 pages. ISBN-978-2-11-152646-4. [consulté le 12 mai 2022]. Disponible à l'adresse : https://sisse.entreprises.gouv.fr/files_sisse/files/outils/fiches/la-securite-economique-au-quotidien-en-28-fiches.pdf

CETISME (Co-operation to promote economic and technological influence in small and medium-sized entreprises) partenariat formé d'iDeTra S.A., Dirección Regional de Investigación - Comunidad de Madrid, du Conseil Régional de Lorraine, de Coventry University Enterprises Ltd et de Consorzio Pisa Ricerche, ATTELOR et Meta Group. Intelligence économique. Un guide pour débutants et praticiens. [en ligne]. 2002. 97 pages. ISBN-84-451-2389-0. Disponible à l'adresse : https://www.madrimasd.org/sites/default/files/intelligence-economique-guide-integral.pdf

MADINIER, Hélène. Haute école de gestion Genève. Intelligence économique. Guide à l'attention des PME de Suisse Romande. [en ligne]. 2ème édition, février 2016 (liens mis à jour en janvier 2017). 35 pages. [consulté le 12 mai 2022]. Disponible à l'adresse : http://www.jveille.ch/wp-content/uploads/2019/02/guide_ie_pme_version_16_17.pdf

DHAOUI, Chedia. Université de Lorraine. Les critères de réussite d'un système d'intelligence économique pour un meilleur pilotage stratégique : Proposition d'un Modèle d'évaluation de la Réussite d'un Système d'Intelligence Économique [en ligne]. Thèse présentée et soutenue le 04 avril 2008. 610 pages. p 547-571. [consulté le 12 mai 2022]. Disponible à l'adresse : https://hal.univ-lorraine.fr/tel-01752721/document

Délégation interministérielle à l'intelligence économique (appelée Service de l'Information Stratégique et de la Sécurité Économique (S.I.S.S.E.) 12 mai 2012. - Diagnostic d'intelligence économique et de sécurité des entreprises (D.I.E.S.E.) [en ligne]. Avril 2014. [consulté le 12 mai 2022]. Disponible à l'adresse : https://sisse.entreprises.gouv.fr/fr/ressources/diese