La Compétitivité Entre L'Intelligence Economique et l'Espionnage Economique

Competitiveness Between Business Intelligence and Economic Espionage

Dr Slimane MRABET *
Laboratoire MECAS, Université de Tlemcen, Algérie
Slimane.mrabet@univ-tlemcen.dz

Received: 24/01/2022 *Accepted*: 15/04/2022 *Published*: 22/04/2022

Résumé :
La monté en puissance de la mondialisation des affaires et la naissance des économies de la connaissance, où l'information est devenue un actif stratégique pour les entreprises, ont rendu l'environnement de plus en plus complexe, instable et difficile à prévoir. Devant ces changements radicaux et pour préserver et améliorer la compétitivité de l'entreprise, l'intelligence économique est devenue un outil incontournable pour le suivi et la surveillance des perturbations ainsi que la détection des signaux annonciateurs de menaces et d'opportunités. L'intelligence économique repose essentiellement sur collecte, le traitement et l'analyse des données à fin de les transformés en informations utiles pour la prise de décisions. Cependant la recherche excessive de l'information et par n'importe quel moyen, à pousser les entreprises et dans de nombreux cas au non-respect des règlementations légales et éthiques de la société, de sorte que l'espionnage économique et informationnel est devenu le pendant illégale de l'intelligence économique. A travers cet article nous essaierons d'expliquer les raisons qui ont fait que l'intelligence économique dépasse ses limites et se transforme en espionnage économique .

Mots clés: Intelligence économique, Espionnage économique, Information, Compétitivité, Veille stratégique.

Abstract :
The rise of business globalization and the birth of knowledge-based economies, where information has become a strategic asset for companies, have made the environment increasingly complex, unstable and difficult to predict. Faced with these radical changes and to preserve and improve the company's competitiveness, business intelligence has become an essential tool for the monitoring and surveillance of disruptions and the detection of signals that herald threats and opportunities. Business intelligence is essentially based on collecting, processing, and analyzing data to transform it into useful decision-making information. However, the excessive search for information, by any means, pushes companies and, in many cases, to the non-respect of society's legal and ethical regulations. As a result, economic and informational espionage has become the illegal counterpart of economic intelligence. In this article, we will try to explain why economic intelligence has gone beyond its limits and has turned into economic espionage .

Key Words: Business intelligence, Economic espionage, Information, Competitiveness, Strategic intelligence.
JEL Classification : L86, M21, M14.
***Key Words*:** Brand, Distinction , Identification, Identity consumption, Loyalty.

Auteur correspondant : Mrabet Slimane *(slimanemrabet@yahoo.fr*)

Introduction :

Du point de vue de l'entreprise, la compétitivité est définit comme la capacité de produire des biens ou des services avec un rapport qualité-prix opportun, ce qui permet à l'entreprise de réaliser une bonne rentabilité tout en gagnant des parts de marché sur ses concurrents nationaux et internationaux.

Or, aujourd'hui le consommateur ne se contente pas seulement du produit, Mais il cherche également les avantages et les services qui y sont associés, Cela conduit l'entreprise à rechercher la compétitivité en dehors des coûts et à travers d'autres éléments tels que l'image de marque, délais de livraison, les services et d'autres éléments qui confèrent à l'entreprise un solide avantage concurrentiel. Néanmoins cette compétitivité est plutôt de l'ordre du moyen et long terme et nécessite des moyens important pour se construire.

Cette compétitivité multi-sources nécessite la mise en place de politiques et de décisions stratégiques qui leur permettent de maitriser la situation. Cependant, la matière première fondamentale de ces politiques et décisions est l'information. Cette nouvelle forme de compétitivité basée sur l'exploitation de l'information fait appel à tout le cycle de l'intelligence économique comme façon de penser et manière d'action

L'intelligence économique nécessite la mise en place d'un système efficace de production de connaissances, dans le but de réduire l'incertitude et la protection du patrimoine informationnel. Cependant la recherche excessive de l'information et par n'importe quel moyen, à pousser les entreprises et dans de nombreux cas au non-respect des règlementations légales et éthiques de la société. De ce fait l'espionnage devient de plus en plus dangereux et destructeur. Bien que le cout de l'espionnage est difficile à évaluer pour différentes raison (Verizon, 2018) la Cybersecurity Ventures prévoit que les coûts mondiaux de la cybercriminalité augmenteront de 15 % par an au cours des cinq prochaines années, pour atteindre 10.500 milliards de dollars US par an d'ici 2025, contre 3.000 milliards de dollars US en 2015. Cela représente le plus grand transfert de richesse économique de l'histoire, et sera plus rentable que le commerce mondial de toutes les principales drogues illégales combinées (Cybersecurity Ventures, 2021). Devant cette situation critique, la légalité et l'éthique sont les deux clés qui feront la différence entre l'intelligence et l'espionnage.

I. Espionnage économique

Maximiser les performances est devenu le challenge de toutes les organisations, tant privées que publiques. Cependant, plusieurs moyens pour parvenir ne respectent pas les réglementations légales et éthiques de la société. La multiplication des affaires d'espionnage ces des dernières décennies révèlent l'ascension du phénomène dans le monde des entreprises et des affaires. Avant d'aborder la définition de l'espionnage, il est nécessaire de bien distinguer les différents termes qui sont employés. L'espionnage économique est un sujet interdisciplinaire sans dénomination standard (Button. M, 2020). Les dénominations actuelles sont très variées, puisqu'elles sont inventées en fonction de différents contextes disciplinaires (sciences économique, sciences politique,

sciences juridiques…etc.). Wang. V et Hou. T Nous présente un lexique de quinze dénominations pertinentes (Wang. V et Hou. T ; 2020). Cependant Il existe actuellement au moins cinq termes génériques très répandus à savoir : Espionnage des affaires (Business espionage), Espionnage d'entreprise (Corporate espionage), Espionnage industriel (Industrial espionage), Espionnage commercial (Commercial espionage), Espionnage économique (Economic espionage) (Wimmer.B, 2015)

Ces cinq termes renvoient tous au même domaine général. Néanmoins le terme l'espionnage économique est souvent utilisé pour faire la différence entre l'espionnage gouvernemental et/ou militaire et l'espionnage pratiqué par les entreprises. Cependant il n'est pas toujours possible de distinguer clairement l'espionnage gouvernemental de l'espionnage commercial, tout simplement parce que le bienêtre économique est étroitement lié à la sécurité national (Wimmer.B, 2015)

D'une manière générale, les termes espionnage industriel, espionnage commercial et espionnage d'entreprise sont tous utilisés lorsque l'espionnage est effectué à des fins commerciales par contre l'espionnage économique est utilisé pour parler de l'espionnage mené par les gouvernements, et il a généralement une portée internationale, cependant il est difficile de Différencier l'espionnage international de l'intra-national.

Pour L. Konstantopoulos l'espionnage économique comporte trois dimensions distinctes; La première, appelée espionnage macroéconomique, fait référence à l'utilisation d'agences secrètes pour le compte du gouvernement d'un État afin d'aider les dirigeants à mener des politiques économique interne et externe avec les meilleurs résultats possibles. La deuxième dimension, appelée espionnage microéconomique, où le gouvernement d'un État par le biais de ses agences secrètes est engagé dans la collecte de renseignements afin d'aider une entreprise (généralement une multinationale) dont le but est de l'emporter sur ses concurrents dans l'arène économique internationale. La troisième dimension de l'espionnage économique est le contre-espionnage économique (counterintelligence) dont le but est l'identification et la neutralisation des services de renseignement étrangers pour préserver l'intérêt national (Konstantopoulos. L, 2006). Par ailleurs Sølen. K. S distingue l'espionnage économique de l'espionnage industriel en expliquant que pour l'espionnage industriel les gouvernements ne sont pas impliqués dans les opérations de collecte d'informations et de renseignement industriel, c'est un espionnage pratiqué par l'entreprise et pour l'intérêt propre de l'entreprise (Sølen. K. S, 2016 ; Wagner. R .E, 2012).

Comme la frontière entre l'espionnage et d'autres pratiques légales comme l'intelligence économique reste floue, Wang. V et Hou. T nous propose les quatre éléments suivant pour faire la différence entre l'espionnage et d'autres pratiques douteuses (Wang. V et Hou. T ; 2020) :

- Méthode - Il s'agit d'un processus de collecte, d'analyse et de gestion systématiques d'informations sensibles et confidentielles, y compris les secrets commerciaux, les informations opérationnelles, la propriété intellectuelle, etc.

- Intention - Son objectif est d'utiliser les informations acquises pour obtenir un avantage concurrentiel au détriment du concurrent ou vendre à des personnes et/ou des groupes intéressés.
- Acteur - Elle est généralement menée par un individu ou une organisation.
- Nature - Il s'agit d'une activité illégale et contraire à l'éthique.

Par espionnage, on entend l'ensemble des actions d'acquisition ou d'interception illicite et illégale de secrets d'affaires ou de savoir-faire des entreprises rivales**,** tenues volontairement confidentielles. Selon Economic Espionage Act of 1996 (E.E.A) l'espionnage économique "is the theft or misappropriation of a trade secret with the intent or knowledge that the offense will benefit any foreign government, foreign instrumentality, or foreign agent" (legal information institute). Le vol d'informations touche directement les secrets commerciaux qui sont définies comme des informations qui tirent des valeurs économiques indépendantes du fait qu'elles ne sont pas facilement connues par les concurrents (Goldstein. P, 2007). Les secrets commerciaux peuvent inclure des formules, des procédés de fabrication, des méthodes permettant d'améliorer la prise de décision, la conception d'un produit ou d'un service…etc. (European Commission, 2018). Rustmann décrit l'espionnage industriel comme une activité cynique, éhonté et sans donner aucune importance à la morale (Rustmann. F. W ,2002), par contre la norme sociale impose au veilleur d'être chaste en adoptant des méthodes et des techniques civilisé et raffinées pour la collecte de renseignement auprès des entreprises (Cornwall , 1991). Dans ce contexte la culture du veilleur et/ou de l'entreprise est un facteur clé qui influe directement sur les perceptions de l'illégalité et de l'éthique en termes de pratiques commerciales (Lacoste. P, 2013)

1. Méthodes d'espionnage industriel

Les méthodes utilisées pour le renseignement et l'espionnage économique sont très variées. Elles vont des simples techniques de collecte d'informations aux méthodes d'espionnage au caractère clandestin indéniable. Les méthodes utilisées par l'espionnage industriel ne sont pas automatiquement illégales et immorales, c'est-à-dire que l'espionnage utilise à la fois des moyen légaux et illégaux. Button.M nous énumère un ensemble d'activités couvertes par le terme générique d'espionnage industriel classées par ordre croissant d'illégalité, à savoir : open source intelligence (renseignement de source ouverte), reverse engineering, hiring employees of competitors, dumpster diving, cultivating insiders, illegal surveillance (la surveillance illégale) and hacking (le piratage) (Button. M, 2020). Cependant, il n'est pas facile de déterminer avec précision la légalité des activités mentionnées ci-dessus, et lorsque la loi n'arrive pas à réglementer des activités compliquées, le volet éthique entre en scène, rendant les choses encore plus confuses et embrouillées (Wang. V et Hou. T ; 2020).

L'intelligence économique, se base sur la collecte de renseignement auprès de source ouverte, appelé information blanche. Cependant l'espionnage industriel essaye d'aller plus loin pour s'approcher de l'information confidentielle appelé information grise et/ou noir. Les formules utilisées sont très variées, la formule la plus proche de la légalité est le reverse engineering. Il consiste à démonter un objet

pour détecter ces secrets, comprendre sa conception et déterminer ces composants afin de le dupliquer ou de l'améliorer et d'écourter le processus de R&D. Le débauchage (hiring employees of competitors) est une autre technique assez répandus dans le domaine des affaires, elle consiste à recruter des employés actuels ou anciens d'un concurrent ou d'une entreprise similaire. Le "Dumpster diving" ou fouiller les poubelles à la recherche d'informations utiles est une autre tactique obscure ; Le Dumpster diving repose essentiellement sur le manque de connaissances en matière de sécurité, de nombreuses choses de haute valeur peuvent être trouvées en fouillant les poubelles (par exemple, des CD, des DVD, des disques durs, des répertoires d'entreprise, etc.) C'est une méthode suspecte et douteuse, avec beaucoup de défiance et de méfiance.

Devant l'incapacité de trouver des solutions d'amélioration de la compétitivité avec les méthodes légale, les managers rivaux optent pour des méthodes illégales basées sur vol de connaissances et le copiage sans autorisation. Avec le développement d'Internet et du Cloud, le hacking ou les cyberattaques sont de plus en plus fréquentes et perfectionnées, il est impossible de deviner ce dont un hacker compétent est capable s'il dispose de suffisamment de temps et de ressources. Beaucoup de multinationales se sont retrouvées à la merci d'un hacker capable de dépasser leurs mesures de sécurité même les plus perfectionnés. Cependant ne pas être connecté, ne constitue pas une barrière pour bloquer l'espionnage industriel. Très souvent, les insiders (ressources humaines internes) prêtes à coopérer avec les espions sont utilisées pour accéder à l'entreprise, même dans certains cas, les employés peuvent eux-mêmes être à l'origine du délit d'information, en proposant la vente des secrets de l'entreprise aux concurrents (Pasternak.G et Witkin.G, 1996) à savoir que 85 % des cas d'espionnage sont commis en coopération avec des insiders (Wang. V et Hou. T ; 2020).

II. Intelligence économique

Le dynamisme perpétuel de l'environnement commercial contemporain rend les entreprises de plus en plus dépendantes d'un système d'information pour la détection précoce des changements afin de pouvoir réagir de manière la plus efficace possible (Kahaner 1996). Cependant L'évolution des technologies de l'information (Hard and Soft) a rendu les activités de collecte, de stockage et de diffusion des informations une tâche très facile. Le problème qui persiste est de savoir comment obtenir des informations utiles et de qualité. Néanmoins Les entreprises ne peuvent disposer d'informations de qualité que si elles instaurent un système intégré et intelligent de collecte et d'analyse des données (Gonzalvo 2015 ; Tuan 2016). Ce système est connu sous le nom d'intelligence économique ou Competitive Intelligence.

Les dénominations actuelles sont très variées et quelque peu floue. De nouveaux termes apparaissent au fur et à mesure que la discipline d'intelligence économique mûrit au sein de l'entreprise. Il existe au moins quatre termes génériques très répandus à savoir : Intelligence Economique (Competitive Intelligence),

Business Intelligence, Market Intelligence and Corporate Intelligence (Global Intelligence Alliance, 2004). Le terme d'intelligence économique (Competitive Intelligence) est le plus utilisé, le plus développé et des plus diffusés dans la littérature (López-Robles et al. 2019a), et considéré comme terme global, qui rassemble la plupart des aspects que l'intelligence économique peut présenter (Heras-Rosas and Juan Herrera, 2021).

En raison de la pluridisciplinarité du sujet il n'existe pas de consensus sur la définition de l'intelligence économique (Pélissier et Nenzhelele 2013), les deux chercheurs nous propose 50 définitions et concluent que l'absence d'une définition universelle a conduit à l'apparition de nombreuses définitions de l'intelligence économique qui diffèrent du fait qu'elles se concentrent sur certains aspects de l'intelligence économique tout en laissant de côté d'autres aspects. Cela signifie que les frontières du domaine de l'Intelligence économique ne sont pas clairement définies.

L'intelligence économique est définit comme "A process or practice that produces and disseminates actionable intelligence by planning, ethically and legally collecting, processing and analysing information from and about the internal and external or competitive environment in order to help decision-makers in decision-making and to provide a competitive advantage to the enterprise" (Pellissier et Nenzhelele 2013). C'est une définition globale qui prend en considération l'ensemble des domaines que touche l'intelligence économique. Néanmoins tous chercheurs essayent de focaliser l'attention sur l'aspect éthique à fin de bien différencier l'intelligence économique de l'espionnage économique. Sous cet angle l'intelligence économique est "An ethical process for obtaining information on the competitive environment " (Weiss and Naylor 2010) et qui utilise des sources publiques (McGonagle et Vella, 2002). Le terme "public" désigne toute information que l'on peut légalement et éthiquement identifier, collecter et ensuite utiliser.

Gelb et Zinkhan (1985) distinguent l'intelligence défensive de l'intelligence offensive. Par intelligence défensive, les entreprises s'efforcent d'en savoir plus sur les concurrents actuels et potentiels, les nouveaux produits, les produits de substitutions, les caractéristiques des produits, les tendances du marché etc. à fin de détecter les points fort des concurrents et de les prendre en considération au moment de prise des décisions. Par contre l'intelligence offensive, se concentre sur l'identification des faiblesses des concurrents dans le but de les utilisés pour tracer des stratégies d'attaque (Gelb et Zinkhan, 1985).

L'intelligence économique repose sur la combinaison de trois fonctions informationnelles fondamentales (Larivet, 2009). Celles-ci se déclinent en veille ou renseignement (Lesca, 2003 ; Harbulot, 2012), en influence ou en lobbying (Huyghe, 2001 ; Larivet 2009) et en protection ou gestion du risque informationnel (Larivet, 2009). Concernant la veille, elle est définit comme l'ensemble des actions coordonnées de recherche, de traitement et de distribution de l'information en vue de son exploitation (Jakobiak. 2004 ; Martre 1994) sans oublier de lier les unes aux autres par une boucle de rétroaction (feedback loop) (McGonagle et Vella, 2002).

L'influence ou le lobbying est la deuxième constituante de l'intelligence économique. L'influence est considérée comme un refus d'accepter l'environnement de l'entreprise comme une contrainte, ses règles et ses lois comme des données (Larivet, 2001). La protection est la dernière composante de l'intelligence économique et qui permet à l'entreprise de se défendre contre les différentes opérations d'intrusion (Bulinge et Moinet 2013).

La veille constitue l'élément essentiel de l'intelligence économique, elle se caractérise par un système informationnel qui vise essentiellement la détection des signaux faibles (Ansoff. 1975) et les alertes précoces (Lesca, 2003) par un suivi intelligent et attentif de l'environnement. Le terme veille est un terme générique qui englobe plusieurs types de veilles. En s'appuyant sur le modèle des cinq forces de Porter (Porter, 1979) Martinet et Ribaut ont développé quatre types de veille, à savoir : la veille technologique, la veille concurrentielle, la veille commerciale et la veille environnementale (Martinet et Ribault, 1987). Cependant La veille est toujours sectorisée en fonction des besoins de l'entreprise, ce qui donne une multiplication des types de la veille (nombre illimité de veille).

La fonction veille impose la participation de tous les acteurs de l'entreprise pour relever les défis de l'écoute intelligente de l'environnement. Vu les besoins informationnels de l'entreprise ainsi que le nombre de sources d'information qui existent, la tâche de collecte d'informations devient de plus en plus accablante. Pour faire face, il est nécessaire d'instaurer une équipe polyvalente en fonction de la taille de l'entreprise (Lackman et al, 2000). Pour Lenz et Engledow (1986) le nombre d'employés dédiés à la fonction d'intelligence économique doit être compris entre un et sept employés. Toutefois la présence d'expert et spécialiste d'informations au sein de l'équipe de veille permet à l'entreprise de construire un système de gestion de l'information structuré et indépendant (Salvetat et Laarraf, 2013).

Au début, la cellule d'intelligence économique était rattachée au département de la planification, mais avec l'accumulation des expériences, les entreprises ont commencées à placer la cellule d'intelligence économique au sein des autres fonctions tel que le marketing, les finances, la gestion des opérations et d'autres fonctions de l'entreprise (Miller, 2000). Notons que l'emplacement de la cellule n'est pas vraiment très important, l'essentiel qu'elle soit proche du centre de décision et qu'elle ne soit pas étouffé par la bureaucratie (Miller, 2000) sans oublié de doter la cellule avec les moyens humain et technologique adéquat.

L'intelligence économique ne remplace pas les études de marché, la planification stratégique, le marketing, l'analyse financière etc. mais elle renforce et soutient la prise de décision dans ces fonctions par le biais des informations collectées et analysées. Ainsi, les out puts de l'intelligence économique constituent un ingrédient incontournable dans la formulation de la stratégie d'entreprise (Rouibah et Ould-Ali 2002).

III. Facteurs contribuant à la propagation de l'espionnage économique

L'espionnage industriel est devenu aujourd'hui l'un des caractéristiques les plus marquantes des pratiques d'intelligence économique malgré son interdiction et sa dangerosité, car l'espionnage est rentable, attrayant et permet facilement de contrôler les concurrents. Afin de montrer l'ampleur de son exacerbation dans la vie économique, nous essayons étudier le phénomène de l'espionnage industriel sous les trois aspects suivants :

- L'antécédent des chercheurs ;
- La terminologie utilisée ;
- le choix du veilleur.

1. L'antécédents des chercheurs

Les actes antérieurs, les faits et les expériences nous permettent de bien comprendre la conduite présente de la personne. Hans Peter Luhn (1896- 1964) est le père fondateur de l'intelligence économique, il a définie l'intelligence économique en 1958 en utilisons le terme de business intelligence (ALTER SI, 2020). En tant que pionnier de la science de l'information, il a travaillé chez IBM comme ingénieur de recherche dans le domaine de l'information et de la bibliothèque (SIB) (Luhn.H.P, 1958) après avoir travaillé comme officier de communication dans l'armée allemande pendant la Première Guerre mondiale. Il fut le premier chercheur avoir réunie entre deux cultures différentes : la culture de la bibliothéconomie et le renseignement militaire (Larivet. S, 2009).

Simon. H (1916- 2001) est Un autre pionnier dans le domaine de la recherche de l'information et la prise de décision, parmi ces innovations le modèle I.M.C de prise de décision, où I : exprime l'intelligence, M : la modélisation et C : le Choix. Concernant l'intelligence, elle est liée à l'exploration de l'environnement afin de détecter les situations qui nécessitent une prise de décision, cette étape liée à la recherche d'informations tire son nom de la terminologie militaire anglo-saxonne (Larivet. S, 2009). Quant à Wilensky. H. L (1967), l'auteur de la plus ancienne définition de l'intelligence économique, il s'est appuyé à son tour dans ses recherches sur les études des services du renseignement américain.

Sur la base de ce qui a été développé, de nombreux chercheurs ont rejeté le terme d'intelligence économique du fait que son origine et sa réputation indiquent la possibilité d'existante d'un lien étroit avec l'espionnage industriel, et ils ont adopté le terme de veille.Outre Simon, Luhn et Wilensky, nous trouvons également Sammon. W. L et All qui se sont appuyés dans leur livre « Business competitor intelligence, methods for collecting, organizing, and using information » (1984) sur un document de l'École du renseignement militaire datant de 1968, ainsi que sur une référence militaire datant de 1973 (Larivet. S, 2009). Un autre chercheur éminent, Tyson. K. W. M qui a développé ses idées à partir de références appartenant au renseignement d'état et sur des manuscrit de la guerre froide. Fuld. L. M est un autre chercheur très distingué dans le domaine de l'intelligence économique, il s'est appuyé sur les travaux de E. Zacharias ; un ancien officier du renseignement de la marine pendant la Seconde Guerre mondiale.

Toutefois, les choses ne s'arrêtent pas là, ce sont les chercheurs eux-mêmes, comme Jakobiak. F (1984), qui conseillent les entreprises de se rapprocher des spécialistes de la défense nationale afin d'en tirer des enseignements utiles sur les « techniques et outilles » de recherche de l'information. Ainsi il réserve une section complète aux institutions de renseignement comme la DGSE, MSS et la CIA.

Nombreux aussi sont ceux qui ont développé leur aptitudes dans les services de sécurité et se sont tournés vers le monde des entreprises, et ils se sont remarquablement distingués par leur précieux travail académique comme Bulinge. F, qui a travaillé dans la police française, comme il l'explique lui-même dans sa thèse de doctorat en sciences de l'information.

Pour démontrer et clarifier encore davantage la grande dépendance de l'intelligence économique envers les services de sécurité, on prend l'exemple de la France, qui fait partie des pays précurseurs en matière d'application de l'intelligence économique, où elle a nommé en 2003 Alain Juillet responsable de intelligence économique, et qui est l'un des vétérans de la direction générale de la Sécurité extérieure (D.G.S.E.).

Tous ces pionniers qui ont imprégné le domaine de l'intelligence économique ont essayé de faire passer leur expérience, savoir et culture d'une façon directe ou indirecte au monde de l'entreprise, chose qui a fait que l'espionnage l'emporte sur l'intelligence dans de nombreux cas.

2. La terminologie utilisée

Fréquemment la recherche scientifique véhicule des termes très répondu et facile à comprendre mais avec beaucoup de nuance de sens et de connotation négative, ce qui permet au côté illégale et non éthique de devancer le côté légale et éthique. Une terminologie dont la circulation se propage rapidement en raison de sa facilité d'emploi. Parmi les dénominations les plus répondu on trouve le terme de guerre économique.

C'est un terme très en vogue, utilisé pour la première fois par Bernard Esambert, le conseiller économique du président français Georges Pompidou (Cohen. G. S, 1991) pour expliquer la situation dans laquelle se trouvait l'économie française, puis s'est propagé dans les quatre coins du monde. Esambert B. (1991) explique que la guerre à de nouvelles armes tel que la compétitivité-cout, l'innovation, la créativité, l'éducation…etc. Le terme a également généré l'émergence et l'utilisation de beaucoup de terme superflus de la même famille comme : attaque, défense, armes, armée, champs de bataille...etc. situation qui peut conduire à des interprétations et des explications qui donnent lieu à des attitudes et des comportements dangereux sur la concurrence et la vie des entreprises.

Nous ne nous s'arrêtons pas au terme "guerre économique", mais il existe autre termes et idées qui font à l'heure actuelle l'objet d'une promotion intense en tant que méthode judicieuse. Parmi les expressions les plus utilisées on trouve les deux locutions « steal with pride » ou « voler avec fierté », et « not-invented-here » ou « pas inventé ici ». Des locutions utilisées pour pousser les veilleurs à être très curieux et beaucoup plus obstiné et agressif dans la recherche, la collecte et le copiage des idées et de l'intelligence des autres. Parmi les exemples les plus

frappants on trouve le livre d'Earls. M (2015), un manuel de règles sur la façon de voler le meilleur de ce que font les autres pour leur propre besoin.

3. Le choix du veilleur

Avec la mondialisation la concurrence s'est intensifiée et l'information est devenue l'input le plus précieux. Cependant, compte tenu de l'immensité du champ de recherche, de la complexité du processus de veille et de la diversité des sources d'information, il est devenu nécessaire pour les organisations d'affecter des veilleurs chevronnés à chacune des forces concurrentielles du marché. Parmi les recrues préférées par les entreprises on retrouve les vétérans de l'armée et de la police, en raison de leurs capacités à mener des enquêtes et de s'infiltrer auprès des centres de décision.

Leur nombre dans la sphère économique augmente de plus en plus grâce à leur expérience acquise au sein de leurs établissements et agences de renseignement. Ce sont les spécialistes de l'informel et de l'infiltration dans les milieux les plus difficiles et les plus renfermé, c'est une catégorie qui a été formée et imprégnée de principes qui leur permettent de pratiquer l'espionnage sans conscience. Abandonner l'espionnage après l'avoir pratiqué pendant une longue période est presque impossible même avec des valeurs éthiques très respectables, tout simplement parce que « l'habitude » dépasse leur volonté. C'est Tout à fait comme le médicament qui fait l'objet de recherches et d'un contrôle strict, mais provoque toujours des effets indésirables immédiatement ou après un certain temps.

Etre sous la dépendance des agents de renseignement police ou militaire et l'utilisation de leur jargon, apporteront inévitablement à l'entreprise des idéologies allochtones. Les veilleurs « espion » essaient toujours de démonter leurs capacités et de proposer des solutions tangibles aux problèmes de l'entreprise. Le danger réside dans la transmission de leur philosophie et mode de pensé à l'ensemble des ressources humaines de l'entreprise, ce qui constitue une menace réelle sur leur intégrité ainsi que sur la concurrence.

Conclusion :

Dans un environnement concurrentiel de plus en plus fondé sur la connaissance, les incitations à dépasser les limites légales et éthiques de la collecte des informations ont augmenté de manière significative. En outre, les limites de la définition des pratiques acceptables sont de plus en plus floues, surtout maintenant que les technologies de l'information et de la communication, les technologies de surveillance et d'autres outils « d'espionnage » sont devenus très facilement accessibles aux entreprises.

L'espionnage économique est largement condamnée par le monde des affaires et réprimé par les institutions des états dans tous les pays du monde, par contre l'intelligence économique se développent et bénéficient chaque jour d'une attention accrue de la part des managers et des décideurs, où les connaissances sont devenues la source la plus importante pour préserver et améliorer la compétitivité des entreprises.

L'espionnage économique ne peut être maitrisé et éloigné du monde des affaires que par une bonne maitrise des facteurs qui d'une façon directe ou indirecte contribues à sa propagation. Le bon choix des responsables de l'intelligence économique qui se distinguent par leur intégrité et leur bonne moralité, ainsi que l'utilisation d'une terminologie scientifiques distinct des termes conduisant à la diffusion des pratiques immorales et illégales, rendront inévitablement l'intelligence économique nettement préférable à l'espionnage économique, et promouvra également la concurrence qui mène inévitablement au développement économique mondial et à la prospérité.

Références Bibliographiques :

- Alter Si (2020) "Business Intelligence : Rappel Historique Et Définition" In https://alter-si.fr/quest-ce-que-business-intelligence/. Last revised 13/06/2021
- Androulidakis I, Kioupakis F.E (2016) "Industrial espionage and technical surveillance counter measures". Springer Avast Academy "Qu'est-ce que le hacking ? " In https://www.avast.com/fr-fr/c-hacker. Last revised 25/10/2021
- Ansof. H. I (1975) "Managing Strategic Surprise by Response to Weak Signals" California Management Review V 18(2). In https://journals.sagepub.com/doi/ 10.2307/41164635. Last revised 12/05/2020
- Bulinge. F, et Moinet. N (2013) "L'intelligence économique : un concept, quatre courants" Sécurité et stratégie 2013/1 (12).In https://www.cairn.info/revue-securite-et-strategie-2013-1-page-56.htm. Last revised 06/04/2020
- Button. M (2019) "economic and industrial espionage" In https://link.springer.com/article/10.1057/s41284-019-00195-5. Last revised 18/11/2021
- Cohen. G. S (1991) "de la guerre industrielle" Dunod
- Cornwall. H, (1991). "The Industrial Espionage" handbook: Century
- Cybersecurity Ventures (2021) "Top 6 Cybersecurity Predictions And Statistics For 2021 To 2025" In https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/. Last revised 14/01/2022
- Earls. M (2015) "Copy, Copy, Copy: How to Do Smarter Marketing by Using Other People′s Ideas" John Wiley & Sons.
- Esambert B. (1991) "La guerre économique mondiale" Éditions O. Orban
- European Commission (2018) "The scale and impact of industrial espionage and theft of trade secrets through cyber" In file:///C:/Users/HP/Downloads/ The%20scale%20and%20impact%20of%20industrial%20espionage%20and%20theft%20of%20trade%20secrets%20through%20cyber%20-%20PwC%20Study.pdf. Last revised 10/10/2021
- Gelb. B. D, Zinkhan. G. M (1985) "Competitive Intelligence Practices of Industrial Marketers" Industrial Marketing Management Revue, V14

- Global Intelligence Alliance (GIA) White Paper (2004) "Introduction to Competitive Intelligence" In file:///C:/Users/HP/Downloads/INTRODUCTION _TO _COMPETITIVE_INTELLIGENCE.pdf, Last revised 25/12/2021
- Goldstein, P. (2007). "Intellectual Property: Tough new realities that could make or break your business". London, England: Penguin Group.
- Harbulot.C (2012) "Manuel d'Intelligence Economique" PUF
- Heras-Rosas.C and Juan Herrera. J (2021) "Innovation and Competitive Intelligence in Business. A Bibliometric Analysis" International Journal of Financial Studies 9: 31.In file:///C:/Users/HP/Downloads/ijfs-09-00031.pdf. Last revised 20/11/2021
- https://www.law.cornell.edu/wex/economic_espionage#:~:text=The%20Economic%20Espionage%20Act%20of,foreign%20instrumentality%2C%20or%20foreign%20agent. Last revised 03/01/2022
- Huyghe. F. B (2001) "L'ennemi à l'ère numérique : chao, information, domination" PUF
- Jakobiak. F (2004) "L'intelligence économique en pratique" Economica.
- Kahaner, L. (1997) "Competitive intelligence: how to gather, analyze, and use information to move your business to the top" Touchstone, New York.
- Lackman. C. L., Saban. K. and Lanasa. J. M. (2000). "Organizing the competitive intelligence function: A benchmarking study," Competitive Intelligence Review, V11
- Lacoste.P (2013) "Espionnage et économie" Revue Cité, 2013/4 N°56. In https://www.cairn.info/revue-cites-2013-4-page-165.htm. Last revised 15/08/2021
- Lacoste.P (2013) "Espionnage et économie" Revue Cité, 2013/4 N°56. In https://www.cairn.info/revue-cites-2013-4-page-165.htm. Last revised 15/08/2021
- Larivet.S (2001) "Intelligence économique : acception française et multi dimensionnalité "In https://www.strategie-aims.com/events/conferences/13-xeme-conference-de-l-aims/communications/2383-intelligence-economique-acception-francaise-et-multidimensionnalite/download. Last revised 20/01/2021
- Larivet.S (2009) "Intelligence Economique : Enquête dans 100 PME" PUF
- legal Information Institute "Economic Espionage" In
- Lenz. R.T. and Engledow. J.L. (1986). "Environmental Analysis Units and Strategic Decision Making: A Field Study of Selected Leading-Edge Corporations," Strategic Management Journal, V7(1).
- Lesca. H (2003) "Veille Stratégique : Méthode le Scanning" EMS.
- López-Robles, José Ricardo, José Ramón Otegi-Olaso, Igone Porto Gómez, and Manuel J. Cobo (2019) "30 years of intelligence models in management and

business: A bibliometric review" International Journal of Information Management 48: 22–38.

- Luhn.H.P, (1958) "A Business Intelligence System" IBM Journal, October 1958. In http://altaplana.com/ibm-luhn58-BusinessIntelligence.pdf. Last revised 25/02/2021
- Martinet. B et Ribault. J.M (1989) "La Veille technologique, concurrentielle et commerciale". Paris, Les Editions de l'organisation.
- McGonagle, J.J. and Vella, C.M. (2002). Bottom line competitive intelligence, Quorum Books, Westport.
- Miller. J.P (2000) "Millennium intelligence: understanding and conducting competitive intelligence in the digital age" Menford, New Jersey, Cyber Age Books
- Pasternak, G; Witkin, G. (1996). The Lure of the Steal. US News & World Report, 45.
- Pasternak, G; Witkin, G. (1996). The Lure of the Steal. US News & World Report, 45.
- Pellissier. R and Nenzhelele. T. E (2013) "Towards a universal definition of competitive intelligence" South African Journal of Information Management 15(2). In https://sajim.co.za/index.php/sajim/article/view/559/666. Last revised 21/12/2021
- Porter. M (1979) "How Competitive Forces Shape Strategy" Harvard Business Review, mars-Avril 1979. In http://faculty.bcitbusiness.ca/KevinW/4800/porter79.pdf. Last revised 01/12/2021
- Rustmann, F.W (2002) "CIA, Inc.: Espionage and the Craft of Business Intelligence" Potomac Books.
- Salvetat. D and Laarraf. Z (2013). "Competitive intelligence key players within firms: the case of high technology European firms," Human Systems Management, V 32.
- Sammon. W. L et All (1984) "Business competitor intelligence, methods for collecting, organizing, and using information" John Wiley & Sons Inc.
- Søilen, K. S. (2016). Economic and industrial espionage at the start of the 21st century–Status question is. *Journal of Intelligence Studies in Business, 6(3).*
- Tuan.L. T (2016) "Organisational ambidexterity and supply chain agility: the mediating role of external knowledge sharing and moderating role of competitive intelligence" International Journal of Logistics Research and Applications. v 19 Issue 6
- Verizon (2018) "Data Breach Investigations Report: 11th edition". In https://www.verizon.com/business/resources/reports/DBIR_2018_Report.pdf. Last revised 15/12/2021

- Wagner. R .E (2012) “Bailouts and the Potential for Distortion of Federal Criminal Law: Industrial Espionage and Beyond” TULANE LAW REVIEW, Vol 86 N° 5. In file:///C:/Users/HP/Downloads/SSRN-id1923469%20(1).pdf. Last revised 15/10/2021
- Wagner. R .E (2012) “Bailouts and the Potential for Distortion of Federal Criminal Law: Industrial Espionage and Beyond” TULANE LAW REVIEW, Vol 86 N° 5. In file:///C:/Users/HP/Downloads/SSRN-id1923469%20(1).pdf. Last revised 15/10/2021
- Wang. V et Hou. T (2020) «Industrial espionage :A systematic literature review (SLR)» In https://www.researchgate.net/publication/343826075_Industrial_Espionage_-A_Systematic_Literature_Review_SLR. Last revised 02/11/2021
- Weiss. A and Naylor. E (2010) “Competitive intelligence: How independent information professionals” American Society for Information Science and Technology 37(1), 30–34. http://dx.doi.org/10.1002/bult.2010.1720370114. Last revised 18/09/2021
- Wilensky H.L. (1967) “Organizational intelligence: knowledge and policy in government and industry” New York, Basic Books Inc., Publisher.
- Wilensky. H. L (1967) “Organizational Intelligence“ Basic Books, Inc., Publishers
- Wimmer.B, (2015) « BUSINESS ESPIONAGE: Risk, Threats, and Countermeasures .In https://dl.acm.org/doi/pdf/10.5555/2843516. Last revised 04/01/2022
- ZaCharias. M (1985) « secret missions: the story of intelligence officer », Putnam 1985.