UNIVERSITÉ DU QUÉBEC À MONTRÉAL

LA CONVOITISE DE L'IMMATÉRIEL À L'ÈRE DE L'HYPERCONCURRENCE : L'ESPIONNAGE ÉCONOMIQUE CHINOIS AUX ÉTATS-UNIS ET AU CANADA

MÉMOIRE
PRÉSENTÉ
COMME EXIGENCE PARTIELLE
DE LA MAÎTRISE EN SCIENCE POLITIQUE

PAR
SIMON PICHÉ-JACQUES

MAI 2021

REMERCIEMENTS

Je souhaite remercier mon directeur de recherche Frédérick Gagnon (professeur de science politique à l'UQAM, directeur titulaire de la Chaire Raoul-Dandurand et directeur de l'Observatoire des États-Unis et de l'Observatoire des conflits multidimensionnels) non seulement pour ses judicieux conseils, son humour, sa patience, son énergie contagieuse et sa passion qu'il partage, mais également pour la chance qu'il m'a donnée en 2019 en me permettant d'agir à titre de chercheur à la Chaire Raoul-Dandurand en études diplomatiques et stratégiques, ainsi que de poursuivre mes travaux.

Je remercie également mes collègues de la Chaire, qui m'ont conseillé et guidé à travers les dernières étapes de ma maîtrise en science politique. Ces personnes font véritablement partie d'un groupe sélect; elles sont talentueuses, rigoureuses et inspirantes. La fin de mon parcours universitaire a été marquée par la rencontre de cette formidable équipe et j'en retire une immense fierté.

Plus personnellement, je voudrais remercier mes parents pour leur soutien indéfectible, particulièrement ma mère, Johanne Piché. Véritable main invisible derrière une grande partie de mes travaux depuis ma première journée d'école, elle a été d'une aide inestimable durant les vingt dernières années. Je n'aurais franchement pas eu le même succès sans sa rigueur, son dévouement et sa très grande curiosité intellectuelle.

AVANT-PROPOS

L'espionnage économique fait l'objet d'un nombre croissant d'études et d'analyses dans le domaine de la sécurité nationale aux États-Unis et au Canada. Dans les deux pays, les ressources dédiées à l'espionnage économique commencent à peine à révéler une prise de conscience de la gravité du problème. Malgré tout, celui-ci demeure peu chiffré et peu connu.

Si l'espionnage devient un phénomène de plus en plus préoccupant mondialement, tant dans le secteur public que privé, il a cependant rarement bénéficié d'une conceptualisation théorique. Une telle conceptualisation permettrait pourtant d'appréhender et de répondre plus efficacement à une problématique dévastatrice pour les entreprises dans les secteurs stratégiques, et pour l'économie des États. Dans une perspective géoéconomique des relations internationales, l'idée nous est donc venue d'écrire sur un enjeu d'actualité qui ne cesse d'inquiéter tant les dirigeants de la fonction publique que les chefs d'entreprise américains et canadiens.

Analyser l'espionnage dans son sens le plus large demeure toutefois un défi considérable. Il s'agit avant tout de pratiques clandestines, dont la majorité des opérations demeurent à ce jour classifiées. Ce jeu de coulisses, protégé sous le sceau de la confidentialité nationale, est en définitive un monde très peu accessible. De plus, le fait de focaliser les recherches sur un pays comme la Chine représente un immense défi langagier, ce qui nous expose au risque de proposer une conceptualisation occidentalocentrée du phénomène étudié. Cette mise en garde est non seulement utile mais nécessaire pour la lecture de ce mémoire.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE D'ABRÉVIATIONS, DE SIGLES ET D'ACRONYMES

2PLA	Second Département de l'Armée populaire de Chine (GSD)
A2/AD	Déni d'accès et interdiction de zone
AMC	Affaires mondiales Canada
APL	Armée populaire de libération
ASFC	Agence des services frontaliers du Canada
CIA	Central Intelligence Agency
CITIC	China International Trust Investment Company
COSTIND	Commission for Science, Technology and Industry for National Defense
CPSNR	Comité des parlementaires sur la sécurité nationale et le renseignement
CSARS	Comité de surveillance des activités de renseignement de sécurité
CSBA	Center for Strategic and Budgetary Assessments
CSIS	Center for Strategic and International Studies
CSSA	Chinese Students and Scholars Association
CSSTI	China Society for Scientific and Technical Information
CST	Centre de la sécurité des télécommunications Canada
DHS	Department of Homeland Security
DIA	Defense Intelligence Agency
DMCA	*Digital Millennium Copyright Act*
DOC	Department of Commerce
DOD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
EEA	*Economic Espionage Act of 1996*
FBI	Federal Bureau Investigation
GAO	Government Accountability Office

GPD	Bureau de liaison du Département des politiques générales
GRC	Gendarmerie royale du Canada
HHS	Department of Health and Human Services
HUMINT	*Human Intelligence*
ICE	Department of Homeland Security's Immigration and Customs Enforcement
IDE	Investissement direct étranger
IMINT	*Imagery Intelligence*
IRCC	Immigration, Réfugiés et Citoyenneté Canada
MASINT	*Measurement and Signatures Intelligence*
MERICS	Mercator Institute for China Studies
MID	Military Intelligence Division
MOFCOM	Ministère du Commerce (en remplacement du MOFTEC)
MOFTEC	Ministère chinois des Relations et du Commerce de l'économie étrangère
MOST	Ministère des Sciences et Technologies
MSE	Ministère de la Sécurité de l'État
MSP	Ministère de la Sécurité publique
NASA	National Aeronautics and Space Administration
NBS	Bureau national des statistiques (National Bureau of Statistics)
NCIX	National Counterintelligence Executive
NCSC	National Counterintelligence and Security Center
NET	*No Electronic Theft Act of 1997*
NRO	National Reconnaissance Office
NSA	National Security Agency
OMC	Organisation mondiale du commerce
OSIF	*Open source Information*
OSINT	*Open source Intelligence*
PCC	Parti communiste chinois

PME	Petites et moyennes entreprises
R&D	Recherche et développement
RPC	République populaire de Chine
S&T	Science et technologie
SCEA	Silicon Valley Chinese Engineers Association
SCIC	Society of Competitive Intelligence of China
SCRS	Service canadien du renseignement de sécurité
SIGINT	*Signal Intelligence*
SSB	Bureau de la Sécurité d'État à Shanghai
SSTIC	Sichuan Scientific and Technical Information Center
TSA	*Trade Secret Act*
USDA	U.S. Department of Agriculture
USTR	United States Trade Representative

RÉSUMÉ

Ce mémoire démontre que les États-Unis et le Canada ne conçoivent pas l'intelligence économique de la même manière que la Chine, et que ces visions divergentes permettent de comprendre en partie les failles du contre-espionnage économique américain et canadien à l'égard des activités clandestines chinoises. Alors que les États-Unis et le Canada perçoivent la Chine sous l'angle de la compétitivité économique, la Chine conçoit sa relation avec ces derniers selon une logique de guerre économique. En raison de son économie développée de façon militaire et patriotique, et de ses fortes ambitions nationales, la Chine est en mesure d'élaborer ses propres stratégies de développement industriel, et mise de façon récurrente sur des opérations clandestines aux États-Unis et au Canada. Misant sur les paradigmes de « guerre économique » et de « compétitivité économique », qui sont tous deux liés au concept d'intelligence économique, nous démontrerons que l'intensification des opérations d'espionnage chinoises aux États-Unis et au Canada depuis les années 1990 est en partie due à une conception canado-américaine de l'intelligence économique différente du modèle chinois.

Mots-clés : Intelligence économique, espionnage économique, Chine, États-Unis, Canada, géoéconomie, guerre économique, concurrence, entreprise, renseignement, information, secteurs stratégiques, technologie, ingénierie inversée, transfert de technologie, propriété intellectuelle

ABSTRACT

This paper demonstrates that the United States and Canada do not see competitive intelligence like China sees it. These divergent visions allow us to understand in part the flaws of American and Canadian counterintelligence practices against Chinese economic espionage. While the United States and Canada both view their respective relationships with China through the lens of economic competitiveness, China consistently perceives these relations from an economic warfare standpoint. As a result of military and economic patriotism, and its national ambitions, China is relying substantially on recurrent covert operations in both the United States and Canada in order to expand its own industrial development strategies. Based on the paradigms of "economic warfare" and "economic competitiveness" within the realm of competitive intelligence, this research will demonstrate that the intensification of Chinese espionage operations in the United States and Canada since the 1990s is partly due to a different Canada-US conception of economic intelligence than that used by China.

Keywords: Competitive intelligence, economic espionage, China, United States, Canada, geoeconomics, economic warfare, competition, intelligence, information, strategic sectors, technology, reverse-engineering, technology transfer, intellectual property

In every operation there is an above the line and a below the line.
Above the line is what you do by the book.
Below the line is how you do the job.

John le Carré
A Perfect Spy

INTRODUCTION

En Chine, les verbes *apprendre* et *imiter* forment un seul et même mot, 学, lequel renvoie à une relation hiérarchique entre le maître et l'élève culturellement et moralement acceptée, voire valorisée. Et si cela tient de la morale et de l'éthique que de s'inspirer du travail de l'autre pour réussir collectivement par l'entremise d'un réseau de partage, le contraire s'observe en Occident, où l'éthique de travail incite davantage à l'ingéniosité individuelle, à la personnalité et à la distinction comme principes de base au succès.

En filigrane des relations internationales, le pillage de la connaissance se poursuit aux quatre coins de la planète, un fléau qui gangrène l'économie des États, et projette à certains égards une dynamique du chacun pour soi. Exacerbée par l'avènement des technologies numériques, la convoitise des États et des entreprises se tourne alors vers le savoir-faire détenu tant par leurs adversaires que leurs alliés, et implique pour plusieurs une reformulation simultanée des concepts de propriété et de sécurité nationale. Cette reformulation entraîne une plus grande porosité entre l'éthique et l'immoralité, précisément entre l'investigation légale et l'espionnage.

L'atteinte au patrimoine immatériel, précisément au savoir technique et aux banques de données détenus par les entreprises et les États, s'avère actuellement un enjeu alarmant pour les firmes et les services de renseignement américains et canadiens. Ces derniers sont de plus en plus préoccupés par la stratégie chinoise d'acquisition illégale de technologies occidentales dans un dessein de modernisation. Aux États-Unis comme au Canada, l'impact des pratiques clandestines chinoises soulève plus que jamais la pertinence d'un partenariat public-privé plus étroit et d'un cadre juridique plus adapté aux nouvelles réalités. Plusieurs se posent alors la question : jusqu'où faut-il pousser la défense des intérêts nationaux dans un contexte concurrentiel où l'espionnage économique tous azimuts est en hausse?

Puisque la Chine cherche à se hisser au faîte des honneurs en matière de science et technologie (S&T) pour conquérir des domaines stratégiques, elle s'est dotée, depuis la fin des années 1970, de mécanismes législatifs et de politiques encore plus explicites pour favoriser la captation d'information confidentielle détenue par l'Occident. Si bien que la Chine est devenue, avec les années, l'un des pays les plus agressifs en la matière. L'information convoitée par la Chine n'est plus strictement rattachée aux domaines militaire et politique; elle réside dorénavant dans tous les domaines imaginables.

C'est à partir des années 1970 que la Chine a commencé à faire sourciller les experts du domaine de la sécurité nationale, mais il a fallu attendre les années 1990 pour que l'espionnage économique chinois finisse par inquiéter les gouvernements américains et canadiens. D'abord, il y a eu le rapport *Sidewinder* – un projet très controversé et mort dans l'œuf – entrepris conjointement en 1996 par le Service canadien de renseignement de sécurité (SCRS) et la Gendarmerie royale du Canada (GRC), qui avait pour but d'évaluer l'ampleur de la menace que représentaient l'acquisition et le contrôle d'entreprises canadiennes par des triades chinoises, des magnats originaires de Hong-Kong ou par les services de renseignement chinois. Quasi simultanément, le Rapport Cox traitait du même genre d'enjeu aux États-Unis en 1999, plus largement des opérations clandestines de la République populaire de Chine (RPC) en sol américain entre les années 1980 et 1990. Depuis, le phénomène a pris une ampleur corrélative à l'évolution des technologies et de la remarquable compétitivité du marché.

Keith Alexander, ancien directeur de la National Security Agency (NSA), affirmait en 2012, que le vol de propriété intellectuelle par les cyberattaques représentait le plus grand transfert de richesse dans l'histoire humaine « *the greatest transfer of wealth in human history* » (Rogin, 2012). En la matière, la Chine est devenue le principal auteur de ce crime économique aux États-Unis (*World Threat Assessment*, 2019 : 5). L'actuel directeur du Federal Bureau Investigation (FBI), Christopher Wray, faisait

également remarquer, le 26 avril 2019 au *Council on Foreign Relations* à Washington D.C., que la Chine représente désormais une importante menace pour l'économie américaine et la sécurité nationale, et a recours à l'espionnage et aux activités de piratage (Wray, 2019). Il ajoutait que la Chine :

> *[have] pioneered an expansive approach to stealing innovation through a wide range of actors – including not just Chinese intelligence services but state-owned enterprises, ostensibly private companies, certain kinds of graduate students and researchers, and a whole variety of other actors working on their behalf* (Wray, 2019)

Au Canada, on observe la même tendance. David Vigneault, actuel directeur du SCRS, affirmait en décembre 2018 à l'Economic Club of Canada que la Chine représente dorénavant le défi le plus important pour le pays et constitue une menace sérieuse pour la prospérité et les intérêts nationaux canadiens (Vigneault, 2018).

Il demeure difficile de mesurer l'impact réel de l'espionnage économique, étant donné la confidentialité, le manque de transparence et le mutisme des entreprises sur le sujet (Porteous, 1993 : 32; Katsuya et de Pierrebourg, 2010 : 347; Crosston, 2015 : 113; Slate, 2009 : 11; Søilen, 2016 : 52; Reid, 2016 : 810). Toutefois, plusieurs estimations plus ou moins précises existent malgré que certains cas d'espionnage n'aient jamais été rendus publics, judiciarisés ou ne sont pas totalement connus des services de renseignement. Néanmoins, ces estimations montrent clairement une croissance soutenue.

À l'ère de l'information et de l'hyperconcurrence du marché, la Chine cherche depuis plusieurs années à se définir comme le futur architecte du paysage techno-industriel, alors que ses convoitises hégémoniques s'appuient sur des pratiques économiques qui transgressent souvent les limites du *fairplay* commercial aux États-Unis et au Canada. Sachant que l'intensification de l'espionnage économique chinois est également la conséquence directe de cadres juridiques inefficaces, tant aux États-Unis qu'au

Canada, ainsi que de pratiques entrepreneuriales inadéquates, nous nous focaliserons davantage sur l'aspect socioéconomique du phénomène, celui qui recouvre les divergences de visions de l'intelligence économique.

La question de recherche sera donc la suivante : qu'est-ce qui explique l'intensification de l'espionnage économique chinois au Canada et aux États-Unis depuis les années 1990[1]? Pour répondre à cette question, nous utiliserons le concept d'intelligence économique. Or, bien que l'intelligence économique soit à la fois un concept théorique et une pratique nécessaire à la stratégie entrepreneuriale dans le monde contemporain, la captation de l'information et l'acquisition de technologies étrangères sont en réalité des pratiques qui évoluent en fonction de la posture stratégique qu'adopte un État en matière de développement économique (Potter, 1998 : 56). Misant alors sur les notions de « guerre économique » et de « compétitivité économique », qui sont tous deux liées au concept de l'intelligence économique, nous tenterons de démontrer que l'intensification des opérations d'espionnage chinoises aux États-Unis et au Canada depuis les années 1990 est en partie due à une conception canado-américaine de l'intelligence économique moins agressive que le modèle chinois.

Alors que nous nous focaliserons sur les divergences de conceptions de l'intelligence économique pour démontrer l'intensification de l'espionnage économique chinois depuis les années 1990, des explications rivales peuvent tout autant apporter des pistes de réflexion pertinentes. D'abord, le nombre grandissant de cas d'espionnage pourrait s'expliquer par une mauvaise gestion entrepreneuriale. En effet, de nombreux cadres américains et canadiens ont tardé à implanter une culture de sécurité au sein de leur

[1] Il n'existe pas de données claires et précises sur l'espionnage économique chinois aux États-Unis et au Canada depuis les années 1990. Comme nous le savons, les données sur ces phénomènes sont souvent parcellaires, puisqu'elles ne sont pas toujours publiques, et parce qu'il n'est pas toujours possible d'attribuer la responsabilité à un acteur spécifique. Bien que certaines données aient été rendues publiques au fil des années, et que nous ayons une idée générale de l'ampleur des dégâts causés par l'espionnage économique, nous ne pouvons démontrer empiriquement qu'il y a bel et bien une intensification de ces activités depuis les trente dernières années. En revanche, nous pouvons déduire que l'espionnage est en hausse selon ce que rapportent les différents rapports gouvernementaux américains et canadiens sur ces questions.

entreprise. Préférant rester muets sur les enjeux d'espionnage pour ne pas affecter leur chiffre d'affaires et leur cote boursière, plusieurs ont ignoré leur vulnérabilité, et sous-estimé les conséquences à plus long terme du vol de propriété intellectuelle. Ensuite, les nombreux cas d'espionnage économique chinois depuis les années 1990 peuvent s'expliquer en partie sous l'aspect juridique. En effet, les cadres juridiques aux États-Unis et au Canada ont été déficients à plusieurs titres, particulièrement en ce qui a trait à la portée extraterritoriale des poursuites judiciaires, ainsi qu'à la définition ambiguë de la notion de propriété intellectuelle. Les cadres juridiques des États-Unis et du Canada ont certes démontré leur aspect punitif, mais ont rapidement dévoilé leurs limites quant à la judiciarisation d'entreprises chinoises subordonnées à leur gouvernement. Enfin, l'intensification des opérations d'espionnage chinoises aux États-Unis et au Canada depuis les années 1990 peut être démontrée depuis la montée en puissance de la Chine et sa volonté de supplanter la puissance américaine d'ici 2049. À titre de puissance révisionniste, la Chine a adopté et continue de préconiser une approche de l'intelligence économique plus agressive que celle du Canada et des États-Unis, comme défenseurs du statu quo.

Ce mémoire sera divisé en trois chapitres. Le premier traitera du concept de l'intelligence économique, notamment de son évolution à travers le temps, mais également de l'environnement informationnel qui a favorisé son essor. Dans ce chapitre, nous comparerons deux paradigmes dominants de l'intelligence économique, soit la « guerre économique » et la « concurrence économique ». Le premier chapitre abordera également les rouages de l'espionnage économique et les différents types d'information collectée par des pays comme la Chine. Le deuxième chapitre se concentrera sur les ambitions nationales de la Chine. Nous montrerons précisément comment la Chine s'y prend en matière de renseignement, de stratégies industrielles et de transfert de technologies. Nous y mettrons également en lumière la modernisation de l'appareil militaire chinois. Lorsque nous aurons survolé les rouages du gouvernement chinois, particulièrement ceux des services de renseignements, il sera

plus aisé d'appréhender les deux grands modèles socioéconomiques qui s'affrontent actuellement sur la scène mondiale, entre d'un côté la Chine, et de l'autre, les États-Unis et le Canada[2]. Le troisième et dernier chapitre portera sur les mécanismes de protection américains et canadiens. Cette partie examinera notamment les faiblesses des mécanismes de contre-espionnage, des cadres juridiques et du modèle socioéconomique face aux activités d'espionnage chinois. De fait, la thèse que nous défendons, selon laquelle les États-Unis et le Canada préconisent et conservent une conception de l'intelligence économique différente du modèle chinois sera davantage éclaircie dans cette dernière partie.

Approche méthodologique

Le mémoire privilégie la comparaison par l'entremise de la méthode de la congruence. Pour ce faire, nous avons procédé à une analyse documentaire de sources primaires et secondaires. Il a donc été question de faire un repérage dans la littérature scientifique, dans différentes revues médiatiques, dans des livres spécialisés, et dans des documents officiels sur le sujet, durant la période choisie. Une recherche documentaire implique également de repérer les ressources informationnelles déjà traitées (revues spécialisées, données statistiques, lois, etc.) pour en retirer des données factuelles afin de répondre à une question de recherche préalable (Laramée et Vallé, 1991 : 157). Nous avons mené une étude qualitative sur l'espionnage, recherché de l'information précise pour chacune des sections du plan de travail et fourni une analyse en fonction des connaissances acquises durant la recension des écrits ciblés. Cette recension a permis de vérifier la

[2] Les États-Unis et le Canada ont une approche de l'intelligence économique qui est semblable. Malgré certaines différences qui pourraient être soulevées, nous avons préféré regrouper les États-Unis et le Canada pour mettre davantage en lumière les différences des modèles avec celui de la Chine.

pertinence d'intégrer la notion d'intelligence économique dans l'analyse de notre problématique (Laramée et Vallé, 1991, *ibid*.).

Sans avoir consulté l'exhaustivité des travaux qui portent sur le sujet, notre travail de recherche brosse somme toute un portrait aussi exhaustif que possible de la situation au Canada et aux États-Unis, ainsi qu'une conceptualisation détaillée de l'espionnage économique. Toutefois, afin d'étudier l'espionnage économique chinois aux États-Unis et au Canada, nous nous sommes essentiellement appuyés sur l'analyse de sources secondaires, particulièrement sur une multitude de publications d'ex-fonctionnaires, de militaires, de journalistes et de chroniqueurs, lesquelles nous sont apparues incontournables pour rédiger ce mémoire. Ces ouvrages nous ont permis d'établir un portrait global de la situation, tant aux États-Unis qu'au Canada, et nous ont, par le fait même, permis d'élaborer plus efficacement le deuxième chapitre, consacré davantage à la structure organisationnelle de la Chine en matière d'intelligence économique.

Nous avons fait des recherches par mots clés, et sélectionné de l'information s'échelonnant de 1990 à aujourd'hui. Nous avons également eu recours (mais pas seulement) à plusieurs périodiques scientifiques. De plus, les ouvrages de Matthew Crosston (2015), Robert Slate (2009), William J. Lahneman (2009), Peter L. Mattis (2012), John Poreba (2012) et Akanksha Vashisth et Avinash Kumar (2013), ont été essentiels pour la rédaction du mémoire, notamment en ce qui a trait au troisième et dernier chapitre consacré à l'impact de l'espionnage économique.

D'un point de vue conceptuel, nous avons décidé d'articuler ce document selon le cadre théorique de l'intelligence économique que proposent Franck Bulinge et Nicolas Moinet dans *L'intelligence économique : un concept, quatre courants* (2013). En se basant sur leur cadre théorique, nous avons choisi de poursuivre dans la même voie et d'appliquer les mêmes concepts pour ce mémoire.

Par ailleurs, puisque l'essence même de notre travail repose sur une théorisation française, de nombreux articles universitaires et journalistiques français ont été

consultés. De fait, les diverses interventions médiatiques d'Alain Juillet, de même que ses travaux des dernières années, ont grandement influencé l'aspect conceptuel de ce mémoire. De la même manière, les travaux de Christian Harbulot (2008) et de Monica Mallowan (2014, 2016) ont guidé notre analyse.

Puisque le concept d'intelligence économique est basé sur une perspective française, la quasi-totalité de la littérature sur le sujet porte sur les services de sécurité nationale de la France. Ainsi, nous avons eu pour défi supplémentaire de vérifier avec la littérature américaine si les prémisses mises de l'avant dans la littérature française étaient compatibles avec les cas américain et canadien. En ce sens, nous nous sommes consacrés également à l'étude du concept américain du *competitive intelligence*, qu'élaborent notamment Craig S. Fleisher et Sheila Wright (2009), Jonathan Gordon-Till (2004), Richard Horowitz (1999), ainsi que Phillip C. Wright et Géraldine Roy (1999).

L'espionnage économique étant une problématique qui devient, avec le temps, une menace à la sécurité nationale, les États concernés sont dès lors les premiers acteurs à condamner ces activités, et donc les premiers à fournir une interprétation. Notre analyse de sources documentaires a donc a été sensible aux biais interprétatifs pouvant se révéler dans la littérature choisie. En somme, le choix d'un corpus de littérature varié a permis de comparer les différences de perceptions de la Chine, des États-Unis et du Canada qui subsistent sur les questions touchant l'acquisition de technologie, la veille technologique, et les principes d'innovation et de modernisation. En mettant en lumière des distinctions politiques, juridiques, administratives et socioéconomiques, les modes opératoires que prescrivent les divers concepts de l'intelligence économique ont permis d'expliquer pourquoi l'espionnage économique chinois est si dommageable aux États-Unis et au Canada, et ce, depuis de nombreuses années.

CHAPITRE I

L'AVANTAGE CONCURRENTIEL : ENTRE VEILLE STRATÉGIQUE, RENSEIGNEMENT ET ESPIONNAGE

L'intelligence, ça n'est pas ce que l'on sait, mais ce que l'on fait quand on ne sait pas.

Jean Piaget

Tout comme l'accélération de la production de masse, du progrès mécanique et de l'accessibilité aux nouvelles technologies générée par les deux premières révolutions industrielles, l'information révolutionne aujourd'hui tous les modes opératoires du système international et transcende le quotidien des organisations étatiques et entrepreneuriales jusqu'à celui du particulier. Si nous parlions à l'époque de la révolution technique par la transformation agricole, l'expansion ferroviaire, la création du moteur à combustion ou la radio, la gestion de l'information a, à son tour, amené le monde dans une nouvelle dynamique, celle de la connectivité, de la vitesse et de l'hyperconcurrence. À l'ère post-industrielle, le désir de connaissance dans le monde est alors passé d'« un besoin diffus à un impératif de survie et de performance, imposé par la course à la compétitivité et à la croissance » (Mallowan, 2014 : 114).

En dépit des bouleversements qu'occasionne la révolution dite de « l'information » (Degaut, 2016 : 509), ses fondements ne sont toutefois pas liés à la puissance énergétique, ni même à ce qui est de l'ordre de la quantité matérielle, mais plutôt à la vitesse et à la cadence (Deschamps et Moinet, 2011 : 149). S'y retrouvent désormais comme véritables changements majeurs « le calcul, la réduction de la marge d'incertitude, la communication en temps réel, la mobilité, l'interopérabilité, le stockage et l'évaluation » (Deschamps et Moinet, 2011, *ibid.*). Bien qu'il s'agisse d'un réel pivot dans les relations sociales, le développement de l'information ne se réduit

pas à un changement historique décisif unidimensionnel. Il bouleverse au contraire, à l'instar des grandes révolutions, toutes les dimensions de la vie humaine, notamment celles de la stratégie et de la politique (Deschamps et Moinet, 2011, *ibid.*).

La révolution de l'information a changé le fonctionnement des économies et jeté les bases d'un monde fondé sur la connaissance (Gurría, 2012). Cette économie, qu'on appelle désormais l'« économie du savoir », implique une accumulation de richesse qui provient aujourd'hui des idées et des innovations qui sont intégrées aux produits et services, si bien que l'avantage concurrentiel des entreprises et des États se retrouve aujourd'hui ancré dans les processus de recherche et développement (R&D), les *softwares* (programmes, logiciels, codage), et les structures organisationnelles et de production, dans ce qui est communément appelé l'« intangible » ou l'« immatériel » (Gurría, 2012). Dans cette conjoncture, l'économie basée sur le savoir se répartit mondialement parmi des pays ayant d'importants écarts de richesse monétaire et des entreprises ayant diverses capacités à bâtir un réseau en matière de R&D (Gurría, 2012).

Dans ce climat mondial de l'information que l'on s'est habitué à nommer « société de l'information », comme le formulait dans les années 1970 le futurologue américain Alvin Toffler, les nouvelles technologies numériques représentent une variable inéluctable : une véritable clef de voûte sociétale. L'environnement informationnel est d'une complexité sans précédent, et oblige le remaniement des structures organisationnelles et la modification de certaines stratégies compétitives, en tenant compte, cette fois, du paradigme de l'information dans leurs approches, afin d'assurer un seuil de performance viable (Mallowan, 2014 : 112). Parce que la parité caractérise désormais le marché mondial, chaque organisation doit tirer son épingle du jeu en misant sur l'avantage de l'information traitée, l'avantage du renseignement.

De cette mouvance résulte un élargissement de la notion du renseignement, affranchie de la représentation simpliste que l'on en faisait durant les deux guerres mondiales et

la guerre froide (Beau, 2010 : 163) La nécessité d'une culture du renseignement est aujourd'hui un élément fondamental aux activités publiques et privées dans les sociétés modernes. Ce faisant, le domaine du renseignement n'est plus strictement rattaché à l'État; il fait intrinsèquement partie de tout environnement stratégique dans lequel résident les notions de concurrence et d'imprévisibilité (Beau, 2010). Autrement dit, le renseignement n'est plus seulement un outil; il doit être un état d'esprit et une préoccupation constante pour toute entreprise ou État œuvrant dans cet environnement international de plus en plus « connecté ».

Ce nouvel état d'esprit devient un impératif dans le contexte où la plus grande perméabilité des frontières, la libéralisation des échanges et les progrès technologiques ont accéléré la création de firmes multinationales dont les ambitions vont de pair avec celles des États. Ces firmes deviennent aujourd'hui parties prenantes de politiques de conquête de marchés extérieurs, ainsi que de contrôle de secteurs stratégiques (Lorot, 2009 : 10). Depuis les années 1970, « la réduction des barrières tarifaires, l'émergence de certains pays, l'inertie des pays occidentaux et le ralentissement économique des pays en développement » ont façonné un monde dans lequel la concurrence est devenue particulièrement « violente » (Juillet, 2020). Cette hyperconcurrence mondialisée encourage les raccourcis économiques et des méthodes qui ne respectent pas toujours l'éthique concurrentielle. Basculant d'emblée dans l'illégalité, l'espionnage n'est jamais hors de portée.

1.1 L'intelligence économique : l'émergence d'un état d'esprit

Élaborée il y a près d'un demi-siècle par les Anglais, « systémisée » ensuite par les Japonais vers le milieu du 20^{e} siècle, et conceptualisée par les Américains dans les années 1980 (Juillet, 2004, cité par Coissard *et al.*, 2010 : 234), l'intelligence économique est, depuis le Moyen-Âge, dans sa forme la plus embryonnaire, une démarche par laquelle il est possible de déceler d'éventuelles menaces et possibilités

par l'exploitation de l'information pertinente (Coissard *et al.*, 2010, *ibid.*). Devenue une véritable culture avec les années, l'intelligence économique se veut un outil de navigation incontournable en raison de la complexité croissante du monde économique. Afin de mieux appréhender le concept, le cas opposant Fusion Systems Corp. à Mitsubishi Electric est particulièrement intéressant.

Au milieu des années 1970, Donald Spero, alors président de Fusion Systems Corp., une firme américaine spécialisée dans la haute technologie, est au cœur d'un litige l'opposant à la compagnie japonaise Mitsubishi Electric. Victime de la stratégie de brevetage japonaise, Spero écrivait ensuite un article à ce propos dans le *Harvard Business Review* en 1990. En voici le résumé :

> Fusion Systems est une PME innovante qui a inventé un dispositif de lampes à ultraviolet. Au milieu des années 1970, elle décide d'entrer sur le marché japonais en vendant son dispositif novateur par l'intermédiaire de distributeurs locaux. Quelque temps après, Mitsubishi Electric achète un exemplaire de ce système et ne tarde pas à déposer une demande de brevet, puis bientôt 300 autres concernant les technologies de lampes à micro-ondes à forte intensité. Près de 10 ans ont passé depuis son entrée sur le marché japonais quand, s'apprêtant à ouvrir une filiale dans ce pays, Fusion Systems Corp. s'interroge sur ces nombreux dépôts de brevet. Que s'est-il passé? L'étude des brevets japonais montre que la tactique de Mitsubishi a consisté à déposer des dizaines de brevets autour de la technique de base du dispositif de lampe à ultraviolet de Fusion Systems Corp. Ce « déluge de brevets » a pour objectif d'accéder à la technologie d'une autre entreprise par des échanges de brevets. L'objectif est de fermer un marché afin d'obtenir une technologie clé (ici la lampe à ultraviolet) en jouant sur les rapports de force et l'encerclement (Macron et Moinet, 2011 : 9-10)

Ce que nous entendons par culture ou état d'esprit, c'est le désir d'ouverture naturelle d'une entreprise pour comprendre son environnement jumelé à une stratégie informationnelle qui se divise en quatre axes : veille stratégique, gestion des connaissances, protection de l'information et influence (*lobbying*) (Mallowan, 2015 : 32). En ce sens, le cas de Fusion Systems Corp. montre clairement ce que l'on tente d'éclaircir ici. Il implique une entreprise japonaise qui surveille son environnement

stratégique (entrée sur le marché japonais de Fusion Systems Corp.), qui travaille en réseau (distributeurs locaux), et qui a ultimement la capacité de retirer un avantage relatif par l'information obtenue et la stratégie de brevetage (Macron et Moinet, 2011 : 10). L'intelligence économique permet aux gestionnaires d'entreprise d'éviter les mauvaises surprises, de prévoir les changements dans les relations d'affaires, de déceler les possibilités et de prédire la stratégie élaborée par la concurrence pour élaborer un plan commercial qui puisse leur être profitable (Juillet, 2014 : 30). L'intelligence économique se veut donc non seulement avantageuse pour une entreprise, mais également pour l'ensemble de la société (Schultz *et al.*, 1994 : 306).

Or, c'est aux États-Unis que la prise de conscience sur l'information comme vecteur de développement économique et social s'est concrétisée le plus (Delbecque et Pardini, 2008 : 18-19). Constatant le rôle charnière que jouait la connaissance technologique dans les sociétés dès la fin des années 1970, les États-Unis ont misé sur la construction d'un réseau national d'information (IST). Ce réseau se basait sur une stratégie d'innovation et de recherche, dont l'objectif primordial était sa diffusion dans toute la communauté scientifique et économique (Delbecque et Pardini, 2008 : 19). Cette mise en réseau s'inscrivait dans un contexte où les États-Unis cherchaient d'abord à préserver une supériorité technologique sur l'URSS, principalement dans les domaines nucléaire et spatial (Delbecque et Pardini, 2008, *ibid.*).

Ce réseau de partage de connaissances reposait sur le concept managérial du *competitive intelligence*, dont les fondements provenaient de la première définition contemporaine écrite en 1968 par l'Américain Harold Wilensky dans son ouvrage *Organizational Intelligence : Knowledge and Policy in Government and Industry*. À cette époque, l'auteur avait plutôt recours à la notion d'« intelligence organisationnelle », et définissait le concept comme une activité de production de connaissances servant les buts économiques et stratégiques d'une organisation, recueillie et produite dans un contexte légal et à partir de sources ouvertes. Des auteurs comme Michael Porter, Craig Fleisher et Babette Bensoussan ont ensuite commencé à employer le terme *competitive*

intelligence, en élaborant une définition plus offensive de l'acquisition d'information à l'égard des concurrents, de renseignements clés et de l'anticipation commerciale de la concurrence. En ce sens, pour Sheila Wright et Jonathan L. Calof, l'objectif de la *competitive intelligence* est : « […] *to better understand customers, regulators, competitors and so forth to create new opportunities and forecast changes in the quest for sustainable competitive advantage* » (Wright et Calof, 2006, p. 454)[3].

Anglicisme et néologisme à la fois, le concept d'intelligence économique a émergé en France dans les années 1990, notamment avec la publication du rapport Martre en 1994, projetant l'intelligence économique au rang de politique publique. Afin de saisir l'importance des facteurs immatériels de la compétitivité, Henri Martre, Philippe Clerc, Christian Harbulot et Philippe Baumard sont parvenus à un consensus sur la définition suivante de l'intelligence économique :

> [Un] ensemble des actions coordonnées de recherche, de traitement et de distribution en vue de son exploitation, de l'information utile aux acteurs économiques. Ces diverses actions sont menées légalement avec toutes les garanties de protection nécessaires à la préservation du patrimoine de l'entreprise, dans les meilleures conditions de qualité, de délais et de coût (Rapport Martre, 1994).

Inspirée de la *competitive intelligence* américaine (Clerc, 2015), l'intelligence économique peut désigner du même coup un corps de doctrines, un champ d'étude, une charte éthique, un concept théorique, une pratique entrepreneuriale ou étatique et une prescription commerciale. Plus largement, le concept français peut se résumer comme un domaine transdisciplinaire qui emprunte le raisonnement et les outils techniques de diverses disciplines, afin de répondre à des tâches transversales (Fougy, 2014 : 3). Autrement dit, l'intelligence économique est à la fois une stratégie d'influence, de communication et de sécurité de l'information, mêlant le travail de veille et la

[3] Bien qu'il existe de subtiles différences entre les concepts pratiques de la *competitive intelligence* et de l'intelligence économique, nous aurons recours, au fil du texte, au terme *intelligence économique* pour jumeler ces deux concepts.

détection. Pour sa part, Alain Juillet définit l'intelligence économique de la manière suivante :

> [Elle] consiste en la maîtrise et la protection de l'information stratégique pour tout acteur économique. Elle a pour triple finalité la compétitivité du tissu industriel, la sécurité économique des entreprises et le renforcement de l'influence [du] pays (Juillet, 2004)

Il faut néanmoins faire la distinction entre la simple gestion stratégique de l'information et l'intelligence économique. La première se définit comme une aide aux décisions en trouvant des appuis dans la veille stratégique et la gestion des connaissances, alors que la deuxième, en plus d'intégrer la veille stratégique et la gestion de connaissances, est teintée de patriotisme, d'une logique de protection, voire de sécurité de l'information et d'influence (Mallowan, 2015 : 35). Dans le contexte où l'économie et la défense nationale sont devenues des secteurs qui se chevauchent et qui partagent parfois une seule et même juridiction, l'intelligence économique recoupe de plus en plus explicitement la notion de sécurité. En ce sens, le terme anglais *intelligence* fait directement référence à une culture opérationnelle et méthodologique qui est propre aux services de renseignement, et signifie littéralement en français *renseignement* (Alloing et Moinet, 2016 : 88).

1.1.1 La production du renseignement

Dans la concurrence économique moderne, l'information que l'on accumule à travers celle-ci devient un avantage comparatif par rapport aux concurrents dans la conquête des marchés (Juillet, 2014 : 30; Coissard, *et al.*, 2010 : 234; Roper, 2014 : 113). Lorsque les entreprises s'équivalent sur le plan technique et industriel, la différence sur le plan informationnel génère d'emblée la création de valeur et devient par le fait même un vecteur de distinction hautement concurrentiel (Juillet, 2019). Il devient alors crucial

pour chaque entité qui évolue dans un environnement compétitif d'adopter une démarche stratégique. Cette démarche sous-entend d'emblée la mise en place d'un processus utile et efficace pour créer du renseignement. Le renseignement est le produit fini de la collecte, de l'évaluation, de l'analyse, de l'intégration et de l'interprétation de données (Roper, 2014 : 102; Katsuya et de Pierrebourg, 2010 : 301).

Pour produire de la connaissance ou du renseignement, on doit s'appuyer sur un procédé méthodologique singulier que l'on appelle le « cycle du renseignement » (Beau, 2010; Bulinge, 2006; Bartes, 2013; Roper, 2014). Bien que le cycle du renseignement soit un modèle qui, en pratique, fait fi de la complexité des organisations (taille, structure, culture, environnement, temps, hiérarchie, etc.) (Bulinge, 2006 : 38), il reste en théorie un modèle empirique intelligible et abouti, servant de base à la création du renseignement. Francois Beau précise :

> Ce processus itératif n'est d'ailleurs pas spécifique de la fonction renseignement, et se retrouve dans de nombreux domaines de l'activité scientifique, du simple raisonnement élémentaire jusqu'à la mise en œuvre de stratégies de recherche beaucoup plus complexes (Beau, 2010 : 166)

Le cycle se décline en cinq étapes :

1- L'identification/expression ou orientation des besoins en matière d'information (Bulinge, 2006) : permet en quelque sorte l'assainissement d'une problématique, notamment en lançant de nouvelles stratégies de recherche.

2- L'acquisition de l'information depuis différents types de sources, ouvertes ou fermées. Les sources ouvertes ou formelles, en anglais : *open source information* (OSIF), correspondent à de l'information accessible à tous (stockage de données, médias sociaux, rapports annuels, journaux scientifiques, études prestataires, brevets, etc.). Cette information peut être transmise par la radio, la télévision ou les journaux, et peut être accessible par l'intermédiaire de bases de données commerciales, d'images ou de dessins techniques (Roper, 2014 : 95). Les sources

fermées ou informelles concernent, pour leur part, de l'information « inaccessible » au public, considérée confidentielle par le détenteur (concurrents, fournisseurs et sous-traitants, candidats à l'embauche, etc.) (CIGREF, 2003 : 46). Cette étape constitue l'élaboration d'un plan de renseignement, lequel permet de mettre au point les tactiques qui seront adoptées.

3- Le traitement de l'information brute par le calcul algorithmique et la comparaison, par exemple (Bulinge, 2006 : 38). Il s'agit d'organiser l'information reçue de manière à optimiser l'utilisation des données recueillies.

4- L'exploitation, la synthèse, l'analyse de l'information. Cette étape correspond à la transformation de l'information en renseignement (Bulinge, 2006).

5- La diffusion du renseignement vers le ou les décideurs concernés (Bulinge, 2006).

Le cycle du renseignement se veut un processus de création de valeur pour une organisation. Cependant, ce cycle se heurte souvent à la réalité, alors qu'en pratique, la collecte d'information n'est pas toujours aussi simple. Résoudre un problème complexe en utilisant ce modèle de veille concurrentielle peut, dans certains cas, corrompre le cycle, voire le mener à l'échec (Bartes, 2013 : 284). La complexité peut s'illustrer par des relations floues entre concurrents, des systèmes de protection hautement sécurisés à l'égard de secrets commerciaux ou des stratégies de désinformation (Bartes, 2013).

Afin d'anticiper les menaces et les possibilités pour assurer et dominer sa part du marché, la production du renseignement est néanmoins ce que toute entreprise doit développer (Hassid et Junghans, 2013 : 1; Bergeron, 2000 : 153). Cette évidence est toutefois un idéal, car bien des entreprises – voire des États – ne tirent pas pleinement profit de la pratique du renseignement, parce que celle-ci est souvent perçue de manière négative (Juillet, 2012). Alain Juillet explique à ce titre que les dirigeants d'entreprise ne voient souvent pas l'intérêt opérationnel d'une telle démarche, puisqu'à la base, ils n'y ont été que faiblement sensibilisés (Juillet, 2012). Il montre, en outre, que dans le monde entrepreneurial, la culture « court-termiste » domine les mentalités, et empêche

un examen adéquat de l'environnement stratégique qui permettrait d'assurer la pérennité économique des firmes. Finalement dit-il, les dirigeants demeurent peu habiles lorsque vient le temps d'élaborer un plan de renseignement efficace (Hassid et Junghans, 2013).

1.1.2 Le « signal faible »

Lorsqu'ils définissent le concept de stratégie de veille concurrentielle, les spécialistes de l'intelligence économique évoquent souvent la notion de « signal faible », pour désigner de l'information qui est très peu « visible », mais riche en valeur stratégique. Voici une analogie utile pour mieux cerner la notion :

> Avant le tsunami qui a frappé l'Indonésie, les côtes du Sri Lanka et du sud de l'Inde, particulièrement dans l'État du Tamil Nadu, ainsi que le sud de la Thaïlande et l'île touristique de Phuket, le 26 décembre 2004, (entre 216 000 et 232 000 morts selon les différentes évaluations), les témoins rapportent que sur la plage, la mer s'est d'abord retirée, mais que les vacanciers sont restés. Ceux qui étaient dans leur hôtel rapportent que des gerbes d'eau ont jailli des siphons des baignoires et des lavabos, mais comment savoir que cela signifie l'arrivée d'une vague de plusieurs mètres qui met sous pression le réseau d'eau? (Lesca et Lesca, 2009 : 139)

Précisément, le signal faible est « un événement apparemment déviant ou insolite, le plus souvent d'apparence insignifiante, et noyé dans une multitude d'autres données plus bruyantes » (Lesca et Lesca, 2009 : 138). Importée de la littérature américaine sur la stratégie et la gestion des entreprises, cette notion a été traitée en 1975 par Igor Ansoff qui se présente comme l'un des premiers auteurs à l'avoir fait. Il la présente comme un élément qui permet de prévoir toute « surprise stratégique », si bien que sa détection fournirait aux décideurs la capacité d'anticiper certains évènements, qui sont en pratique quasi indétectables (Alloing et Moinet, 2016 : 88).

En théorie, l'interprétation d'un signal faible pourrait donc potentiellement fournir des renseignements importants sur un événement imminent. À l'instar des services de renseignements et des divers corps policiers qui effectuent un travail de repérage pour déjouer un attentat terroriste, par exemple, l'intelligence économique prescrit, toute juridiction gardée, le même genre d'écoute anticipative d'évènements annonciateurs d'une atteinte grave (Alloing et Moinet, 2016 : 86). En pratique, par contre, la détection de ces signaux ne se dissocie pas de l'interprétation subjective : « [Ils répondent] à une intentionnalité, un regard et une attention qui ne peuvent être que subjectifs » (Alloing et Moinet, 2016 : 89).

Voir avant tout le monde ce que les autres n'ont pas encore vu est souvent impossible. Le concept opératoire du signal faible évolue dans le champ de la prospective, mais il est difficilement applicable au champ de la surveillance, parce que cela induirait que la veille stratégique est une pratique rationnelle, détachée de tout biais cognitif (Garcias-Nunes et da Silva, 2018 :1). En réalité, « surveiller » suggère une prise de décision préalable, un choix ontologique et une interprétation de l'environnement (Alloing et Moinet, 2016, *ibid.*; Garcias-Nunes et da Silva, 2018 : ibid.). Alloing et Moinet précisent :

> Le fait est que dans la communauté professionnelle du renseignement (au sens large, c'est-à-dire incluant les professionnels de la veille et de l'intelligence économique), les signaux faibles vont devenir un mythe, c'est-à-dire un ensemble de croyances et de représentations idéalisées autour d'un objet, puis d'outils de captation, et partagées par un groupe qui renforce son identité à travers lui (Alloing et Moinet, 2016, ibid.)

Plus théorique que pratique, la focalisation sur le signal faible en intelligence économique corrompt en quelque sorte la démarche efficace de la veille concurrentielle en attribuant une trop grande importance à la recherche au détriment des compétences interprétatives. Cette réalité est encore plus vraie dans les organisations hiérarchiques, alors que le rapport Martre soulignait expressément que : « l'action d'une structure

centralisée ne produit pas l'intensité de connaissances suffisante pour l'appréhension effective d'environnements complexes, ni ne permet sa diffusion rapide » (Martre, 1994, cité par Alloing et Moinet, 2016 : 91). Il ne suffit donc pas uniquement « d'écouter », mais d'être en mesure de pouvoir qualifier une situation. Or, qualifier une situation ne se détache pas non plus d'un raisonnement subjectif antérieur.

1.1.3 Entre éthique et illégalité : la zone grise de l'intelligence économique

Aujourd'hui, de 80 à 90 % de toute l'information existante dans le monde est disponible sur Internet pour quiconque sait les chercher (Roper, 2014 : 94). Certains prétendent que le chiffre s'élève même à 95 % (Juillet, 2020). Comme nous l'avons évoqué un peu plus tôt, l'information se classe en fonction de sa difficulté d'obtention, ainsi que par la valeur qu'elle possède. D'abord, il y a l'information « blanche », ouverte ou formelle, se voulant essentiellement de l'information à valeur moyenne qui est accessible à tous, comme les journaux, les médias sociaux, les rapports annuels, etc. (Juillet, 2020; Decloquement, 2014; Assens et Perrin, 2011 : 140). Ensuite, on trouve l'information « grise », qui est de l'information dont la distribution est restreinte, comme des rapports publiés en peu d'exemplaires, des articles qui exigent un abonnement ou même une conversation entendue (Decloquement, 2014; Assens et Perrin, 2011, *ibid.*). Finalement, il y a l'information « noire », fermée, informelle ou cachée, qui est inaccessible au public et gardée secrète par ses détenteurs, étant donné sa grande valeur stratégique (Juillet 2020; Decloquement 2014; Assens et Perrin, 2014, ibid.). Habituellement, l'information noire implique le domaine des technologies émergentes et les processus de R&D (Roper, 2014 : 133).

Dans l'ensemble, l'intelligence économique ne se base, en théorie, que sur l'acquisition légale de l'information, et exige donc qu'elle se focalise uniquement sur l'information libre d'obtention : l'information blanche et l'information grise, le cas échéant (Juillet

2020; Decloquement 2014). Le fait d'accaparer de l'information noire est alors considéré comme illégal et, en l'occurrence, cette pratique est strictement réservée au domaine de l'espionnage. Autrement dit, l'espionnage survient lorsque les fabricants et les développeurs de produits passent de la simple recherche sur la concurrence à la surveillance intrusive (Roper, 2014 : 111).

Toutes les organisations recueillent de l'information sur leurs proches concurrents, (Crane, 2005 : 234; Schultz *et al.*, 1994 : 308; Vashisth et Kumar, 2013 : 83; Roper, 2014 : 11) en utilisant par exemple la numérisation du marché, le profilage industriel, ou même plus simplement, le *débriefing* de gestionnaires recrutés depuis la concurrence (Crane, 2005 : 234). Ces activités de collecte légales sont devenues des pratiques standardisées dans les études de marché conventionnelles et de l'étalonnage concurrentiel (*benchmarking*) pour assurer un rendement efficace, afin d'en tirer un avantage comparatif (Crane, 2005 : *ibid.*; Katsuya et de Pierrebourg, 2010 : 301). Mais voilà qui démontre la fragilité des assises de l'intelligence économique sur le plan opératoire. Il s'avère qu'il existe « une ligne mince » entre ce qui est de l'ordre de l'intelligence économique et de l'espionnage à caractère économique (Crane, 2005 : 233; Gordon-Till, 2004 : 17; Roper, 2014 : 11).

Les membres de la Strategic and Competitive Intelligence Professionals (SCIP) appellent cette distinction la « zone grise ». Elle constitue un espace où les actions menées par des entreprises peuvent être soit éthiques soit non éthiques, soit même les deux à la fois, selon les circonstances, le cadre éthique utilisé et le système de valeurs organisationnels (Gordon-Till, 2004, *ibid.*). Jonathan Gordon-Till ajoute que dans certains contextes, l'action non éthique n'est pas forcément illégale pour une entreprise, comme cacher son identité réelle dans le cadre d'une entrevue avec un employé concurrent ou payer un ancien employé pour divulguer de l'information sur un concurrent (Gordon-Till, 2004, *ibid.*). « La pratique montre en effet que la tromperie est tout à fait permise, même parfois anticipée », préviennent Norman Schultz, Allison Collins et Michael McCulloch (Schultz *et al.*, 1994 : 308). Puisque l'adversaire ne

s'attend pas à toujours recevoir la vérité, ils ajoutent : « there is no general duty to tell the truth all of the time » (Schultz *et al.*, 1994 : 308).

Profitant des interstices sémantiques de l'intelligence économique, voici les pratiques d'entreprise les plus courantes, recensées par Andrew Pollard dans son ouvrage *Competitor Intelligence* (1999) (Cité de Gordon-Till, 2004, 17-18), pour acquérir un avantage concurrentiel :

- poser des questions camouflées aux employés des concurrents au cours de réunions techniques (utilisées par 78 % des répondants);
- interroger les ex-employés des concurrents au cours d'une entrevue (66 %);
- écouter les conversations entre les employés des concurrents (65 %);
- appeler les fournisseurs et distributeurs des concurrents en faisant semblant de faire une étude sur l'ensemble de l'industrie (55 %);
- prendre des photos ou filmer des travaux d'usines, de bâtiments ou de bureaux des concurrents (52 %);
- se faire passer pour un étudiant de cycle supérieur travaillant sur sa thèse (51 %);
- embaucher un employé loin d'un concurrent afin d'obtenir des renseignements ou un savoir-faire précis (44 %);
- payer un consultant qui a travaillé pour un concurrent pour obtenir de l'information (39 %);
- donner à un employé concurrent une entrevue d'embauche simplement pour obtenir des renseignements (31 %);
- embaucher un enquêteur professionnel pour obtenir des informations précises (29 %);
- aller à une entrevue d'embauche chez un concurrent seulement pour y soutirer de l'information (28 %);
- entrer en négociation avec un concurrent pour obtenir une licence permettant le transfert d'information confidentielle (25 %);
- payer un employé retraité d'un concurrent en échange d'information (23 %).

Toutes ces pratiques sont légales, mais ne respectent pas nécessairement l'éthique entrepreneuriale. Ainsi, l'éthique et la légitimité demeurent des termes discutables selon les points de vue. Bien des actions tombent dans le giron de l'intelligence économique, et soulèvent un véritable questionnement à savoir si cette dernière n'est

parfois qu'un concept permettant de faire bonne figure, afin de mieux dissimuler des pratiques clandestines. Car, en marge des recherches légitimes sur les performances de la concurrence, se trouvent en coulisses, des comportements jugés illégaux, comme le vol de plans de conception ou la recherche de documents stratégiques dans des conteneurs à recyclage (Treviño et Weaver, 1997 : 62). Charlotte Lepri souligne que ce genre de pratique devient de plus en plus courant dans le domaine privé, et ajoute :

> L'espionnage des activités économiques constitue aujourd'hui une dimension essentielle de l'activité d'agents privés. Ce phénomène se développe de deux manières. D'une part, les grandes entreprises développent en leur sein des filiales dédiées aux activités de renseignement. D'autre part, les sociétés d'intelligence économique, les cabinets de consultants ou les sociétés de sécurité se multiplient, proposant leurs services en matière de collecte, d'analyse et de traitement de l'information aussi bien à des sociétés privées qu'aux services de l'État (Lepri, 2008 : 51)

Par ailleurs, chaque environnement possède ses propres structures et normes formelles qui influencent considérablement la façon dont les parties prenantes perçoivent les enjeux en matière d'éthique, de même que les pratiques adoptées pour acquérir un avantage concurrentiel (Treviño et Weaver, 1997 : 68; Slate, 2009 : 7). La concurrence étant perçue différemment selon les milieux, plusieurs la considèrent comme une « guerre », alors que d'autres y voient, en revanche, un environnement plus coopératif, s'approchant du « jeu » (Treviño et Weaver, 1997, *ibid.*).

1.2 Les paradigmes dominants de l'intelligence économique

Il existe de nombreuses définitions de l'intelligence économique, mais aucune ne fait véritablement consensus parmi les experts (Fleisher et Wright, 2009 : 250). Au fil des ans, plusieurs chercheurs et praticiens ont tenté de la conceptualiser, mais la complexité de la réalité s'est constamment érigée en obstacle, rendant alors difficile « l'énonciation

de modèles normatifs acceptés de tous » (Bulinge et Moinet, 2013 : 56). Le constat est clair : les définitions qu'on lui a attribuées au départ semblent trop restrictives pour correspondre parfaitement à sa dimension pratique. En d'autres termes, « l'intelligence économique n'est pas ce qu'elle est censée être. Elle est toujours plus que cela : émergeant comme une construction sociale au sein de l'organisation, elle est ce qu'on en fait » (Bulinge et Moinet, 2013 : 56). La démarche de l'intelligence économique serait intimement rattachée à l'environnement culturel dont elle émerge et au sein duquel elle évolue. Dès lors, la mise en place d'une démarche d'intelligence économique, renfermant la surveillance et l'influence du marché, ferait face à plusieurs enjeux éthiques basés sur des fondements culturels (Fougy, 2014 : 12).

De fait, Franck Bulinge et Nicolas Moinet ont tenté de modéliser le concept d'intelligence économique depuis une perspective constructiviste, en y proposant quatre paradigmes/courants qui exercent une influence sur les démarches entreprises par les praticiens (Bulinge et Moinet 2013 : 2). Il en ressort : la guerre, la sécurité, la compétitivité et la diplomatie économiques (Bulinge et Moinet, 2013 : *ibid.*). Nous nous focaliserons toutefois sur deux paradigmes précis : la guerre économique et la compétitivité économique, lesquels sont selon nous, les paradigmes les plus pertinents pour analyser de manière comparative les politiques d'intelligence économique de la Chine d'un côté, et des États-Unis et du Canada de l'autre.

1.2.1 La « guerre économique » : patriotisme, confrontation et néomercantilisme

« Les puissances s'affrontent de nouveau au grand jour pour la maîtrise des sources d'énergie, la conquête des marchés ou le contrôle des innovations technologiques. », affirment Christian Harbulot et Alice Lacoye (Harbulot et Lacoye, 2008 : 73). Telle est la prémisse de la guerre économique; elle s'impose comme étant « la poursuite de la guerre par d'autres moyens » (Bulinge et Moinet, 2013 : 57). À l'instar de l'école de

pensée réaliste en Relations internationales, le concept de guerre économique nous renvoie aux politiques de puissance des nations. La convoitise des gouvernements n'est cependant plus simplement focalisée sur l'acquisition de terres, mais sur la construction d'un potentiel technologique et industriel (Delbecque et Harbulot, 2011 : 2). La notion de guerre économique s'inscrit dans le discours sur l'intelligence économique en empruntant une vision patriotique des relations économiques. Elle s'érige en opposition à la perspective libérale et avance que les échanges n'offrent pas toujours un résultat gagnant-gagnant (Laïdi, 2016 : 439). En ce sens :

> Dans une compétition, il y a toujours un gagnant et un perdant : un vendeur qui ne parvient pas à vendre et un acheteur qui ne décroche pas un marché. À l'échelle d'un pays, c'est la même chose : certains pays ne trouvent ni vendeur ni acquéreur. Un marché gagné par l'américain Boeing est un marché perdu pour l'européen Airbus. Et vice versa (Laïdi, 2016, *ibid.*)

La guerre économique est un concept qui émerge à la fin de la guerre froide et qui s'appuie sur une vision basée sur la montée en puissance des entreprises par rapport aux États (Laïdi, 2016 : 441). Laïdi soutient que trois raisons expliquent pourquoi la notion de guerre économique trouve alors une grande adhésion. La première réside dans le fait qu'il n'y a plus d'ennemi commun, la deuxième, dans l'émergence de nouveaux acteurs sur la scène internationale, et la troisième, dans une concurrence de plus en plus forte pour la conquête des ressources naturelles (Laïdi, 2016 : 440). Ce phénomène étant observé, la guerre économique se matérialise entre autres sous la forme d'opérations d'espionnage économique (Delbecque et Harbulot, 2011 : 42). Ainsi, dans une logique militarisée et hiérarchisée de l'intelligence économique, la guerre économique illustre une notion se limitant aux relations interétatiques, proposant une grille de lecture pertinente aux activités d'espionnage économique chinois. De la même façon, l'intelligence économique devient en quelque sorte l'outil auquel les États ont recours pour pouvoir évoluer dans une dynamique économique conflictuelle.

Pour les tenants du paradigme de la guerre économique, il s'agit de concevoir l'intelligence économique à travers le prisme de la conflictualité et de la violence. Pour les dirigeants d'entreprises occidentales qui adoptent une démarche d'intelligence économique, très peu la bâtissent sur de tels fondements, car le paradigme de la guerre économique repose quasi uniquement sur la variable interétatique, donc ultimement, sur une subordination du domaine privé à l'État (Bulinge et Moinet, 2013 : 58). En effet, dans le triptyque conceptuel *État-entreprise-puissance*, que Bulinge et Moinet associent à la métaphore *guerre-régiment-soldats* (Bulinge et Moinet, 2013, *ibid.*), la dynamique économique occidentale dépeint une réalité axée sur la dérégulation économique et financière et donc, peu compatible avec des politiques néomercantilistes.

Popularisé par Adam Smith en 1776, le concept du mercantilisme est une doctrine économique et politique développée dans les pays d'Europe occidentale entre 1500 et 1800 dans laquelle les hommes d'État, les décideurs et les commerçants cherchent à accroître la richesse par l'action de l'État (Yu, 2017 : 1044). Prônant de surcroît la subordination de l'économie privée aux objectifs nationaux, le mercantilisme traduit une politique de construction nationale par l'intermédiaire d'un État fort et l'appui des forces armées (Yu, 2017 : 1045). Le pragmatisme inhérent au mercantilisme, réunissant les objectifs du *roi*, du *fonctionnaire* et du *marchand* en un seul but commun, se retrouve encore, à l'époque contemporaine, dans un concept renouvelé que l'on désigne par « néomercantilisme ». Dans l'histoire, explique Fu-Lai Tony Yu, les nations asiatiques qui ont réussi à adopter le néomercantilisme sont le Japon (à l'ère Meiji, 1868-1912), la Corée du Sud, Taiwan et Singapour dans les années 1960 (les nouveaux pays industrialisés), et la Chine contemporaine à l'époque de la mondialisation (Yu, 2017 : 1048). Par conséquent, alors que la Chine favorise une telle approche économique (étatiste), le paradigme de la guerre économique devient pertinent dans la mesure où l'espace de référence des deux concepts est la nation et les valeurs qui y sont véhiculées ont le même dénominateur commun, celui du patriotisme.

Le paradigme de la guerre économique recouvre donc plusieurs notions, dont la prémisse qui repose sur le fait que « tout événement économique [est] envisagé comme la conséquence d'une stratégie appuyant la politique de puissance des nations » (Bulinge et Moinet, 2013 : 57). Entrevoir l'intelligence économique sous l'angle de la guerre économique engendre *a posteriori* des pratiques comme la sécurité active, la contre-ingérence, le renseignement et l'espionnage, l'influence, la propagande et la déstabilisation (Bulinge et Moinet, 2013, *ibid.*).

1.2.2 La « compétitivité économique » : performance, innovation et néolibéralisme

S'appuyant sur une logique libérale, la compétitivité économique préconise une lecture davantage axée sur la conquête de marchés, la compétitivité et l'innovation des entreprises (Bulinge et Moinet, 2013, p. 60). La compétitivité économique met donc de l'avant une perception de la réalité liée aux risques et aux possibilités, en priorisant une posture stratégique qui se focalise sur la rentabilité et la performance d'une entreprise. Dans un environnement mondialisé, le paradigme entrevoit l'intelligence économique comme un vecteur de développement de l'information soutenu en partie par l'État (Bulinge et Moinet, 2013, *ibid.*).

Dans sa posture plus concurrentielle que conflictuelle, la compétitivité économique accorde une importance fondamentale à la veille technologique, notamment en ce qui a trait aux brevets et à la veille concurrentielle afin de rester compétitive. De même, cette notion autorise, voire favorise dans un esprit déontologique, l'obtention de procédés conçus par une autre entreprise. Sans tomber dans les pratiques d'espionnage, la notion de compétitivité économique se sert de l'intelligence économique comme un outil de prise de décision, dans un environnement où l'entreprise est certes l'acteur principal, mais qui est d'emblée entourée d'une pluralité d'acteurs. Dans ce système, les laboratoires et les consommateurs, ainsi que les firmes concurrentes sont mises en

relations, interviennent et influencent le processus innovant des entreprises (El Haoud, 2011, p. 177).

La compétitivité économique est le courant dominant en Occident, et la plupart des acteurs politiques et économiques y font référence, afin d'orienter leurs pratiques d'intelligence économique (Bulinge et Moinet, 2013 : 59). Le courant tire sa légitimité d'un environnement économique dérégulé, et trouve son sens dans une économie de marché où l'initiative individuelle, la propriété privée et la performance (profit) sont tous des éléments qui y sont constitutifs. En théorie, la compétitivité économique s'exprime de façon similaire au cycle du renseignement, un cycle itératif qui repose sur l'équation suivante : *information = compétitivité* (Bulinge et Moinet, 2013 : 60). En pratique, par contre, la réalité montre que l'information n'est pas garante d'une prise de décision qui réduit les incertitudes, alors qu'elle n'est qu'un élément parmi d'autres dans un processus décisionnel (Bulinge et Moinet, 2013, *ibid.*).

La compétitivité économique n'est applicable que dans une situation où les décideurs ont préalablement intériorisé une culture du renseignement (Bulinge et Moinet, 2013, *ibid.*), ce qui suggère en filigrane la mise en place de véritables réseaux (internes et externes), dans lesquels est favorisée une excellente gestion de la communication entre toutes les parties prenantes. En somme, d'une perspective individualiste doit en émerger le culte du partage. En ce sens, il semble que la compétitivité économique soit une perspective plus prescriptive que praticable, dans la mesure où elle simplifie considérablement l'environnement stratégique, et prétend apporter aux entreprises une solution durable dans un contexte d'hyperconcurrence.

Par ailleurs, celle-ci implique une maîtrise de la mondialisation par la promotion du néolibéralisme (Bulinge et Moinet, 2013 : 62). Cette promotion s'articule de manière à encourager une économie de marché par les libertés individuelles et la performance économique. Dans son orientation politique, un effacement progressif du secteur public se manifeste au profit d'une émergence marquée du secteur privé dans le jeu de la

concurrence. La compétitivité économique génère en bout de ligne des pratiques comme la veille technologique, le *lobbying*, le *benchmarking*, etc. (Bulinge et Moinet, 2013 : 59).

Ainsi, lorsque l'on compare la guerre économique à la compétitivité économique, il est clair que les deux paradigmes ne sont pas conciliables. Comme le conclut Bulinge et Moinet : « la posture d'intelligence économique résulte moins du choix d'un individu que d'une adaptation collective à la culture et aux valeurs de l'entreprise » (Bulinge et Moinet, 2013, *ibid.*). L'intelligence économique est donc un concept qui dépend manifestement d'une conception culturelle propre à un milieu donné (Bulinge et Moinet, 2013, *ibid.*). Or, ces deux grilles d'analyse permettent de saisir la logique dans laquelle se trouve un État ou une organisation face aux problèmes qu'engendre la violence des rivalités économiques mondiales.

Si l'on compare maintenant la perspective américaine (libéralisme économique) à la perspective chinoise, on constate qu'il existe des divergences fondamentales en ce qui a trait aux niveaux de développement, ainsi qu'au fonctionnement de leurs institutions économiques respectives. Leur approche en matière de normes et de politiques d'innovation diffèrent nettement (Dieter, 2011 : 2). Pour ainsi dire, les États-Unis sont unanimes quant aux rôles des forces du marché et du secteur privé comme étant essentiels à l'innovation et à la normalisation des relations économiques. *A contrario*, la Chine maintient l'idée qu'il est primordial de compter sur le gouvernement pour définir des objectifs stratégiques, ainsi que pour déterminer les paramètres de régulation économique (Dieter, 2011, *ibid.*). Or, si la Chine est aujourd'hui intégrée à bien des égards dans le système mondial, elle n'est pas plus transparente et responsable; elle a élaboré au fil des années des politiques et des pratiques ciblant le savoir technico-scientifique détenu par les pays occidentaux, afin de l'obtenir clandestinement.

1.3 L'atteinte au patrimoine immatériel en pleine croissance

« Cessons d'être naïfs : dans cette lutte pour la compétitivité et la survie économique il n'y a pas d'amis, il n'y a que des ennemis, car chacun voit midi à sa porte », écrivait Alain Juillet dans le quotidien français d'information économique et financière *Les Échos* (Juillet, 2011). Les cibles ont changé avec la parité mondiale grandissante. Entre, d'un côté, la forte croissance des entreprises en matière de R&D et, de l'autre, les grandes multinationales qui ceinturent le marché avec la multiplication de brevets, l'atteinte au patrimoine immatériel est en hausse, et n'est pas un incident fortuit de l'hyperconcurrence mondiale (Juillet, 2011). Aux États-Unis, par exemple, environ 90 % (21 trilliards de dollars US) de la valeur totale des entreprises S&P 500 résident dans les secrets commerciaux et la propriété intellectuelle (Johnson, 2020). Ces atouts vitaux pour l'État sont devenus la cible d'attaques de plus en plus persistantes, tant par des employés, que des ex-employés, des concurrents, des entrepreneurs, des espions professionnels, des pirates informatiques indépendants, des vendeurs, des consultants en intelligence économique, ainsi que des groupes mandatés par des gouvernements étrangers (Fitzpatrick et *al.*, 2004, cité par Pacini *et al.*, 2008 : 121). La distinction sur le plan économique se fait dès lors dans un espace où l'acquisition d'information sur l'adversaire est hautement favorisée, pour assurer un environnement commercial des plus avantageux.

À la fois « actif intellectuel » et « propriété intellectuelle », le « patrimoine immatériel » inclut donc les banques de données, l'information sur les réseaux d'entreprises, les listes de clients, etc. Le champ des actifs intellectuels abrite entre autres des inventions, des nouvelles technologies, des nouvelles marques, des logiciels, des procédés uniques, etc. (Office de la propriété intellectuelle du Canada, s.d.). Les moyens visant à protéger ces actifs sont, par exemple, les brevets, les marques de commerce, les droits d'auteur, etc. (Office de la propriété intellectuelle du Canada, s.d.). Or, dans le contexte où les entreprises évoluent à l'intérieur d'un réseau, dans

lequel existe le travail en collaboration nécessaire à leur réussite, le cyberespace devient la courroie de transmission qui aide à la diffusion d'information sensible parfois relative à la propriété intellectuelle (Cidon, 2015).

Bien des coups font partie des rivalités économiques. En revanche, ils ne se veulent pas tous permis pour autant. Chacun opte pour sa stratégie, et les risques dépendent de la recette choisie. Lorsque les brevets, les fichiers, les données sur les employés ou les courriels internes sont pris pour cible, le gardiennage de l'entrée principale d'une entreprise, par exemple, devient un moyen de sécurité largement dépassé. Si au siècle dernier, l'avantage comparatif des entreprises reposait plus largement sur l'acquisition matérielle, les mesures de protection allaient en ce sens : surveillance des manufactures et des bureaux pour prévenir les vols de produits, de plans ou de machinerie (Juillet, 2014 : 30). Aujourd'hui, les menaces ont changé, ce qui nécessite la conceptualisation de nouvelles méthodes de protection.

Ce qui est étonnant et à la fois paradoxal, c'est que même si la numérisation des données permet une certaine dissimulation, voire un plus grand sentiment de protection par rapport à l'information stockée dans l'infonuagique (*cloud computing*), une entreprise est de plus en plus exposée au vol de données, ainsi qu'aux activités de cyberpiratage (Juillet, 2014; Roper, 2014 : 113). Ce paradoxe est dû aux faibles coûts qu'engendrent l'exploitation de la cyberpiraterie, mais principalement au fait que la caractérisation de ces nouveaux risques devient difficile à établir. En d'autres termes : « les attaques peuvent être ciblées contre tout type d'entreprise, provenir de n'importe quel pays dans le monde et être menées tant par un groupe organisé que par un individu isolé » (Juillet, 2014). De plus, il arrive bien souvent qu'une entreprise n'ait pas été informée d'une cyberattaque perpétrée contre elle et lorsqu'on s'en aperçoit, il est souvent trop tard (Crosston, 2015 : 113), d'autant plus qu'aucune loi n'oblige les entreprises à rapporter l'incident aux autorités (Grabiszewski et Minor, 2019 : 269). Par ailleurs, la capacité de reconnaître et de comprendre une cyberattaque n'est pas une compétence courante dans le monde entrepreneurial (Crosston, 2015, *ibid.*).

Le cyberespace est un environnement parallèle et invisible qui permet de stocker une énorme quantité d'information, qu'elle soit confidentielle ou non. Il en résulte un espace riche en ressources auquel les acteurs malveillants peuvent, de façon relative, accéder aisément (Buchan, 2019, *ibid.*). Qui plus est, les données sauvegardées dans le cyberespace peuvent être soutirées à distance (hameçonnage/*phishing*) et de manière anonyme, ce qui confère peu de risque à l'espionnage d'une entreprise (Buchan, 2019, *ibid.*; Søilen, 2016 : 52). Ce genre de menace peut provenir d'employés ou d'ex-employés, de pirates informatiques, de sous-traitants de confiance, de partenaires commerciaux, d'universitaires, etc. (Slaterry, 2018 : 18). Dans le rapport de Verizon de 2018, on constate que dans tous les secteurs confondus, la plupart des cyberattaques sont des actions dites « opportunistes », c'est-à-dire menées sans grande planification. Dans le domaine manufacturier, cependant, 86 % des actions ont requis une planification. Parmi celles-ci, 47 % des infractions recensées impliquait le vol de propriété intellectuelle afin d'acquérir un avantage comparatif (*Data Breach Investigations Report*, 2018 : 5)[4].

Le ciblage de la propriété immatérielle détenue par les entreprises et les États est un problème récurrent et croissant depuis de nombreuses années. Dès 2000, le Computer Security Institute et le FBI indiquaient dans une étude que 75 % des 563 entreprises recensées affirmaient avoir enregistré des pertes financières dues à des brèches dans leur réseau de sécurité (Morris, *et al.*, 2000 : 165). De manière exhaustive, 16 % des entreprises ont indiqué que ces brèches ont été causées par des employés sans autorisation, 14 % concernait le vol de secrets commerciaux et 12 % ont été signalées comme une fraude financière (Morris *et al.*, *ibid*.).

Rares sont les entreprises qui n'ont pas souffert de ce genre de problème à un moment ou à un autre (Sinha, 2012 : 38). Par exemple, aux États-Unis, l'*Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* de 2008 dévoilait

[4] Cette étude s'est basée sur 53 308 incidents, impliquant 2 216 violations de données, dans 65 pays différents, grâce à la contribution de 67 entreprises.

que le FBI avait ouvert 55 nouveaux dossiers, que le Department of Homeland Security's Immigration and Customs Enforcement (ICE) avait procédé à 158 arrestations et avait obtenu 187 actes d'accusation qui ont abouti à 143 condamnations pour des infractions pénales liées à l'exportation (ONCIX, 2008 : 1). Ces chiffres ne correspondent toutefois qu'à une partie de la réalité : « les cas où la perte par incidents en dollars est assez grande pour qu'une entreprise dépose une plainte d'espionnage et assume le coût d'enquête qui y est associé », visent, en règle générale, les grandes entreprises qui possèdent une technologie de valeur considérable (Sinha, 2012 : 38-39). Dans le cas où les pertes par incidents ne permettent pas de justifier l'ouverture d'une enquête criminelle, l'affaire tombe à l'eau et ne figure pas dans les statistiques (Sinha, 2012 : 39).

1.3.1 L'intensification du vol de l'intangible : la conséquence d'une nouvelle ère

Le vol d'information a été, et continuera d'être au cœur des dynamiques économiques et des rapports de force étatiques. À la différence, cette fois, des nouvelles technologies qui génèrent une vitesse d'exécution qui exacerbe aujourd'hui cette réalité de façon phénoménale. L'essence même du vol d'information demeure toujours la même : détenir un avantage stratégique et compétitif sur l'adversaire (Podszywalow, 2012; Slate, 2009 : 14). Le vol de l'immatérialité en soi n'est donc pas l'épiphénomène d'une nouvelle ère que l'on pourrait imputer à la révolution de l'information. Voici un exemple historique qui démontre la continuité du vol de l'information stratégique :

> La « première » route de la soie configurait un immense réseau commercial reliant la Chine à la Syrie médiévale – devenue la Turquie – par lequel transitaient, autant de produits marchands que d'idées et moyens techniques. Par l'élaboration de multiples routes terrestres et maritimes, la Chine a longtemps bénéficié du monopole de la production de la soie, et ce, pendant des centaines d'années, alors que la soie avait une valeur se rapprochant de celle de l'or, sinon la dépassant (Podszywalow, 2012). Les voleurs de secrets étaient

> évidemment fortement sanctionnés lorsqu'ils étaient découverts, si bien que la Chine exécutait plusieurs voleurs durant cette période (Podszywalow, 2012, Strategic Direction, 2012)[5]
>
> Vers 300 après J.-C., deux moines nestoriens de l'Église de l'Orient, affectés à une mission évangélique en Inde, ont foulé le sol chinois et ont réussi à dérober secrètement à la Chine des œufs de vers à soie en les faisant passer dans des cannes de bambou. Soutenue par l'empereur byzantin Justinien 1er, cette expédition clandestine, qui aura duré environ deux ans, a permis à l'Empire romain d'acquérir, au bout de plusieurs années, le monopole de la soie en Europe, ainsi que la part du marché qui était rattachée. En bout de ligne, l'Europe a fini par freiner les retombées économiques générées par l'exclusivité de la production de la soie, détenue par la Chine depuis le quatrième millénaire avant J.-C. (Podszywalow, 2012)[6]

Hormis la vitesse et l'utilisation des nouvelles technologies, deux autres éléments engendrent une intensification du vol de l'intangible à l'échelle mondiale : la mondialisation et l'augmentation de la connectivité entre les nations (Crosston, 2015 : 106) En effet, avec la fin de la guerre froide et la fin des hostilités entre les deux grands blocs idéologiques de l'Est et l'Ouest, on observe un appétit grandissant pour l'espionnage économique, ainsi que la diversification des moyens employés pour mener des opérations d'espionnage (Crosston, 2015, *ibid.*; Macodrum *et al.*, 2001 : 139). Cet intérêt économique s'est inscrit dans une perspective selon laquelle le fait de ne pas suivre une économie en voie de mondialisation rapide condamnerait probablement un État, non seulement à des difficultés économiques, mais l'exposerait

[5] Traduction libre

[6] Willy Shih, professeur à l'université Harvard, propose une perspective historique sur ce genre de comportement clandestin en mettant en lumière, à différentes époques, le même genre d'opérations conduites par les Américains (au Royaume-Uni), les Russes, les Allemands de l'Est, les Japonais et les Coréens. De ce constat, Shih en tire la conclusion que l'espionnage semble être une activité de développement tout simplement banale en matière de concurrence industrielle (Strategic Direction, 2012 : 30). En effet, au 19e siècle, l'industrie du textile britannique était particulièrement ciblée par les États-Unis (Voir le cas de Francis Cabot Lowell et du vol de la machine à tisser). Le même genre d'opération s'est produit des siècles auparavant, lorsque les Britanniques, par l'entremise de l'East India Company, ont volé 20 000 pousses de thé dans les provinces chinoises de Fujian et Jiangsu (Fialka, 1997 : xi-xiv, cité par Melanie Reid, 2016 : 823-824).

également à la guerre, à l'occupation, à la perte de territoire, etc. (Crosston, 2015, *ibid.*). Comme l'indique le rapport de l'IP Commission de 2013 :

> […] today's economic world is far more interconnected and operates at a far higher speed, with product cycles measured in months rather than years. Companies in the developing world that steal intellectual property from those in the developed world become instant international competitors without becoming innovators themselves (IP Commission, 2013 : 10)

Ce faisant, le vol de l'intangible s'intensifie dans un tournant mondial majeur, illustrant le passage des sociétés à une économie de l'immatériel. Le champ de bataille original n'est plus nécessairement d'ordre guerrier, mais plutôt économique. La conflictualité directe ou traditionnelle « ne prévaut plus entre les pays développés, [toutefois] les logiques d'affrontement régissant leurs rapports n'en ont pas pour autant disparu. Seuls leur nature et leurs instruments ont changé » (Lorot, s.d., : 111). En ce sens :

> […] the main battlefield is economic rather than military; sanctions are taking the place of military strikes, competing trade regimes are replacing military alliances, currency wars are more common than the occupation of territory, and the manipulation of the price of resources such as oil is more consequential than conventional arms races. The world is witnessing what Edward Luttwak called the rise of geo-economics, a contest defined by the « grammar of commerce but the logic of war » (*World Economic Forum*, 2015 : 4)

Dans un contexte globalisé et globalisant, l'intérêt politique national devient graduellement subordonné aux objectifs économiques. Cette nouvelle dynamique atteste aujourd'hui un important tournant dans les relations internationales, celui d'une entrée dans l'ère des rivalités géoéconomiques (Lorot, s.d., : 110). Par des politiques de conquête de marchés extérieurs et par la prise de contrôle de secteurs d'activité considérés comme stratégiques, un solide engagement des États envers les entreprises nationales en résulte dans certains pays (Lorot, s.d., *ibid.*).

En matière de sécurité nationale, Robert Gates, ancien directeur de la Central Intelligence Agency (CIA), faisait le constat, il y a près de 30 ans, que l'étude des enjeux de sécurité nationale suggère dorénavant une analyse grandement influencée par la dimension économique. À l'occasion d'un discours prononcé à l'Economic Club of Detroit en 1992, il mentionnait que « le réexamen de la sécurité nationale met en lumière l'augmentation spectaculaire de l'importance des affaires économiques internationales en tant qu'enjeu de renseignement » (Cité par Lepri, 2008 : 34). Ceci étant dit, l'intérêt des services de renseignement pour les enjeux économiques n'a jamais véritablement été ignoré (Lepri, 2008, *ibid.*). Il a été rapidement compris que les impératifs liés au domaine de la sécurité nationale s'étendent non seulement à des objectifs purement régaliens, mais également à des considérations rattachées à la prospérité économique, d'où le lien intrinsèque entre sécurité économique et sécurité nationale (Roper, 2014 : 153).

1.3.2 L'espionnage économique : raccourci rentable et universalisé

L'espionnage est protéiforme. Il peut être politique, militaire, économique ou industriel. Les moyens de collecte sont tout autant variés (Katsuya et de Pierrebourg, 2010 : 305), et se divisent en cinq catégories de source d'information :

> 1. Le renseignement par sources humaines (HUMINT), impliquant tant les techniques clandestines que légales, comme le *debriefing*, la photographie, la collecte de données, etc. (Roper, 2014 : 104) Le HUMINT provient d'individus agissant seuls ou supervisés/dirigés par une tierce personne. Dans l'imaginaire collectif, le HUMINT fait souvent référence à l'espionnage, mais en réalité, la pratique démontre que ce type de collecte de renseignements s'effectue par des « collecteurs » qui ne sont pas nécessairement sous couverture, comme les diplomates et les attachés militaires, par exemple (Roper, 2014 : 106).

2. Le renseignement électromagnétique, par multiples formes d'interception technique (SIGINT) impliquant de l'information dérivée des communications, d'un radar ou par télémétrie (Roper, 2014, *ibid.*). La collecte d'information SIGINT peut se faire depuis des navires, des avions, des sites clandestins, des satellites, etc. (Roper 2014 : 107).

3. Le renseignement de mesures et de signatures (MASINT), qui implique de l'information scientifique et technique obtenue entre autres par analyses quantitatives et qualitatives de données métriques, spatiales, nucléaires, optiques, acoustiques et sismiques (Roper, 2014, *ibid.*).

4. Le renseignement par imagerie (IMINT), impliquant les images aériennes et terrestres (Roper, 2014, *ibid.*). « Imagery can be derived from visual photography, radar sensors, infrared sensors, lasers, and electro-optics. IMINT includes the exploitation of data to detect, classify, and identify objects or organisations » (Roper, 2014 : 108).

5. Le renseignement par sources « ouvertes » (OSINT), qui relève de toute l'information rendue publique sous forme imprimée ou électronique (Roper, 2014, *ibid.*).

Ensuite, les diverses formes d'espionnage dépendent de l'auteur et de la nature des renseignements (Buchan, 2020 : 143). Par exemple, Russel Buchan définit l'espionnage politique comme « state-sponsored theft of confidential information, and its purpose is to shed light on the capabilities and intentions of other state and nonstate actors. » (Buchan, 2020, *ibid.*). L'espionnage économique, pour sa part, est également commandité par l'État, mais implique le vol de secrets commerciaux détenus par des

sociétés étrangères, « usually with the intention of passing this information to domestic companies so that they possess a competitive advantage » (Buchan, 2020, *ibid.*)[7].

Le FBI définit concrètement l'espionnage économique comme :

> Economic espionage is foreign power-sponsored or coordinated intelligence activity directed at the U.S. government or U.S. corporations, establishments, or persons, designed to unlawfully or clandestinely influence sensitive economic policy decisions or to unlawfully obtain sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies. This theft, through open and clandestine methods, can provide foreign entities with vital proprietary economic information at a fraction of the true cost of its research and development, causing significant economic losses (FBI, s.d.)

Le National Counterintelligence and Security Center (NCSC) définit l'espionnage économique de manière encore plus précise ici :

> Espionage means (a) stealing a trade secret or proprietary information or appropriating, taking, carrying away, or concealing, or by fraud, artifice, or deception obtaining, a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; (b) copying, duplicating, downloading, uploading, destroying, transmitting, delivering, sending, communicating, or conveying a trade secret or proprietary information without the authorization of the owner of the trade secret or proprietary information; or (c) knowingly receiving, buying, or possessing a trade secret or proprietary information that has been stolen or appropriated, obtained, or converted without the authorization of the owner of the trade secret or proprietary information (NCSC, 2018 : 2)

L'espionnage économique permet aux entités étrangères d'acquérir clandestinement des renseignements économiques vitaux, et ce, à une fraction du coût du processus de R&D (FBI, s.d., *ibid.*; Buchan, 2020 : 144). Ces raccourcis causent non seulement

[7] Il existe également des différences à l'intérieur même de l'espionnage à caractère économique. D'abord, il y a l'espionnage économique s'inscrivant dans une perspective étatique (État c. État), visant également les entreprises. Ensuite, il y a l'espionnage industriel, qui est une pratique s'établissant dans une relation purement privée (compagnie c. compagnie) (Katsuya et de Pierrebourg, 2010, p. 132).

d'importantes pertes financières pour les entreprises visées, mais elles peuvent également entraîner leur fermeture définitive, étant donné leur incapacité à demeurer concurrentes sur le marché, et ce, face à leurs propres idées. Le SCRS réitère : « L'espionnage peut entraîner une perte de revenus pour les entreprises et l'État, des pertes d'emplois et une baisse de compétitivité » (SCRS, 2019). Ces pratiques ont connu une intensification sur la scène mondiale depuis la fin de la guerre froide, et se sont aujourd'hui universalisées[8]. À ce titre, Michel Juneau Katsuya et Fabrice de Pierrebourg soulignent avec justesse :

> La domination des marchés et des zones d'influence est toujours la même, mais les moyens pour tirer son épingle du jeu ont transformé les rivalités guerrières en stratégies de marketing nationales et de conquête des marchés internationaux. Puisque les lois ordinaires du marché économique ne suffisent plus pour se donner l'avantage nécessaire, plusieurs pays se sont rapidement résolus à obtenir des informations stratégiques, voire de voler ou de neutraliser les avancées techniques de la compétition à l'étranger (Katsuya et de Pierrebourg, 2010, p. 132-133)

L'espionnage économique est autant diversifié qu'il s'est exponentiellement complexifié et accru depuis les années 1990. Comme l'énonce Klaus Solberg Søilen, en une dizaine d'années : « we have moved from break-ins *à la Watergate* to theft by hacking » (Søilen, 2016 : 61). Or, les techniques de base de la collecte restent généralement les mêmes : demandes d'information, exploitation de sources ouvertes, demandes d'achat ou de partage de technologie, etc. (ONCIX, 2008 : 2). L'*Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* de 2008 indiquait que certaines entreprises étrangères, soutenues par leur État, sollicitent des relations d'affaires avec les entreprises américaines, qui permettent en retour d'accéder

[8] Dans les années 1990, le SCRS possédait une liste exhaustive des États qui avaient recours à l'espionnage économique au Canada. Sur cette liste figuraient l'Argentine, le Brésil, la Chine, la Corée du Nord, la Corée du Sud, Cuba, l'Espagne, les États-Unis, la France, l'Iran, l'Iraq, Israël, le Japon, les Philippines, la Russie, Taïwan et le Vietnam (Katsuya et de Pierrebourg, 2010, p. 135).

à des projets classifiés (ONCIX, 2008, *ibid.*). L'acquisition par des États mandataires (*proxies*), la présence à des conférences, conventions et foires commerciales ainsi que le ciblage d'information par l'entremise de délégations étrangères en visite dans des installations gouvernementales ou privées, afin d'établir un partenariat de recherche, figurent également dans la liste des activités fréquemment observées (ONCIX, 2008, *ibid.*)[9].

Lorsqu'un lien de confiance s'établit entre des individus, des entreprises ou des gouvernements, la collecte de l'information se fait de façon tant variée qu'ingénieuse (Katsuya et de Pierrebourg, 2010 : 300). Outre l'utilisation de technologies de pointe afin de dérober des secrets commerciaux, l'espionnage économique fait également appel à des stratégies beaucoup moins coûteuses. « Low-tech devices such as neck-ties with hidden cameras […] audio bugs and removable storage devices can all play their part when companies want to bend the rules » (Podszywalow, 2012), la plupart de ces gadgets sont facilement accessibles sur le Web, et ce, à faible coût (Podszywalow, 2012). Il en est de même des télécopieurs, une technologie jugée archaïque, qui est

[9] Carl Roper donnait l'exemple des visites guidées dans les usines, une pratique qui a progressivement cessé de façon concomitante avec les allégations d'espionnage économique qui ont défrayé les manchettes ces dernières années. Il expliquait qu'aux États-Unis, plusieurs usines ont cessé d'organiser des visites publiques, car des ingénieurs et des spécialistes dans des domaines précis pouvaient en apprendre énormément. Par exemple, beaucoup d'information stratégique peut être collectée, comme le type d'équipement utilisé, les produits chimiques mélangés, les formules chimiques produites, etc. « May US factories have stopped giving tours. From a public tour, engineers and specialists in a given subject area can learn a lot. Certain types of equipment do certain things. Knowing what equipment is on the product line and what machinery is used to mix certain types of chemicals or powders in a formula for something help immensely in determining exactly what you are producing. Product X, for example, requires a mixing of seven different powders and three liquids. Certain machinery is necessary. The powders might have to be mixed in certain proportions in a given order. If a person watches a full cycle, timing the flow of the various powders give relative percentage amounts of each. This same is true for liquids when the approximate flow can be determined. Through observation of the boxes or bags of the powders and liquids, the observers may exactly know what product items are being mixed. It won't take a couple of scientists and chemist long to determine the exact formula » (Roper, 2014 : 129).
Ce *modus operandi*, fait écho à un cas qui s'est produit dans une compagnie (pas nommée) spécialisée dans l'alliage de tuiles de céramique pour les moteurs à réaction. À l'occasion d'une visite, des ingénieurs chinois avaient dissimulé des aimants dans la semelle de leurs chaussures et dans leur cravate afin de pouvoir récolter des échantillons de métal tombés sur le sol (Katsuya et de Pierrebourg, 2010 : 298-299).

pourtant, encore aujourd'hui, l'une des sources de fuite d'information (Podszywalow, 2012).

Si l'espionnage économique est protéiforme, il est également multidimensionnel. Alors que nous avions soulevé un peu plus tôt la surveillance physique d'un immeuble comme solution désuète aux différentes formes que revêt l'espionnage d'aujourd'hui, miser uniquement sur le développement de moyens technologiques pour se prémunir contre les actes d'espionnage est aussi peu efficace. Ira Winker, ancien directeur adjoint de la National Security Agency (NSA) souligne dans son ouvrage *Spies Among Us*, que l'information existe dans quatre dimensions ou formats : le papier, le visuel, l'oral et l'électronique (Cité par Podszywalow, 2012). Tous ces « canaux » informationnels sont la cible des professionnels de l'espionnage, par lesquels il est possible de soutirer de l'information (Podszywalow, 2012).

1.3.3. Les secteurs stratégiques ciblés

Dans les pays avancés technologiquement, de nombreux secteurs et domaines sont continuellement ciblés par l'espionnage économique, comme l'aérospatial, la biotechnologie, la chimie, les télécommunications, la cyber-ingénierie, l'exploitation minière et la métallurgie, le nucléaire, le pétrole, l'industrie pharmaceutique, etc. (Porteous, 1993) Cependant, une nouvelle tendance semble se dessiner depuis plusieurs années, celle du ciblage de technologies à double usage (Crosston, 2015 : 106). Les technologies à double usage sont des technologies civiles qui ont un potentiel militaire, et qui deviennent la convoitise de plusieurs États, que ce soit pour acquérir un avantage concurrentiel marqué, gagner des années de coûts liés à la R&D, améliorer les ressources militaires ou avoir la possibilité de court-circuiter des systèmes informatiques rivaux. D'ailleurs, comme l'énonce le National Counterintelligence Center dans son rapport de 2000 : « the pervasive spread of technology with dual

applications (economic and military) is increasingly problematic and offers a powerful incentive for countries to actually intensify their investment and resources on soft spying » (Cité par Crosston, 2015, *ibid.*).

La liste des secteurs et technologies jugés stratégiques par le NCSC montre clairement que l'espionnage économique n'affecte pas uniquement le revenu net d'une entreprise et sa position boursière, mais également la sécurité nationale (Crosston, 2015 : 106-107). Selon le rapport du NCSC de 2018 intitulé *Foreign Economic Espionage in Cyberspace*, les principales industries et technologies ciblées dans l'économie américaine étaient les suivantes (NCSC, 2018 : 11) :

- Énergie et énergie alternative
    - Réacteurs avancés à eau sous pression et centrales nucléaires à haute température refroidies au gaz
    - Biocarburants
    - Industries à haut rendement énergétique
    - Pétrole, gaz et méthane de houille
    - Réseaux électriques « intelligents »
    - Technologies de l'énergie solaire
    - Éoliennes

- Biotechnologie
    - Dispositifs médicaux avancés
    - Biofabrication
    - Biomatériaux
    - Produits biopharmaceutiques
    - Organismes génétiquement modifiés
    - Traitements de maladies infectieuses
    - Nouveaux vaccins et médicaments

- Défense
    - Systèmes aérospatiaux et aéronautiques
    - Systèmes d'armement
    - Systèmes marins

  - Radars
  - Technologies optiques

- Protection environnementale

  - Systèmes de batterie
  - Appareils économes en énergie
  - Matériaux de construction écologiques
  - Voitures hybrides et électriques
  - Gestion des déchets
  - Systèmes d'assainissement (eau et air)

- Fabrication haut de gamme

  - Impression 3D
  - Robotique avancée
  - Moteurs d'avions
  - Secteurs de maintenance et services aéronautiques
  - Avions civils
  - Moteurs électriques
  - Équipement de fabrication de base
  - Machines à commande numérique par ordinateur haut de gamme
  - Matériaux composites
  - Matériaux d'étanchéité
  - Équipement de fabrication de circuits intégrés et technologies d'assemblage
  - Infrastructures spatiales et technologies d'exploration
  - Caoutchouc synthétique

- Technologies de l'information et des communications

  - Intelligence artificielle
  - Analyse des mégadonnées (*Big Data*)
  - Industries électroniques de base
  - Services de commerce électronique
  - Logiciels
  - Puces informatiques haut de gamme
  - Internet des objets (IdO)
  - Équipement de réseau

- Réseaux de communication sans fil à large bande nouvelle génération
- Informatique et communications quantiques
- Matériaux de terres rares

Le rapport du NCSC mettait en lumière une kyrielle d'autres menaces susceptibles de perturber les industries stratégiques. Par exemple, l'infiltration dans les chaînes d'approvisionnement est un problème courant qui continue de menacer les infrastructures critiques et les secteurs clés de l'économie (NCSC, 2018 : 12). De la même manière, les politiques agressives de plusieurs sociétés d'État posent également une menace de plus en plus importante.

CHAPITRE II

LA SUPRÉMATIE CHINOISE PAR L'ACQUISITION DE TECHNOLOGIES OCCIDENTALES

Que celui qui est volé ne s'aperçoive pas
du larcin, qu'il n'en sache rien,
et il n'est pas volé du tout.

William Shakespeare

« Au 21e siècle, si un pays ne parvient pas à être parmi les meilleurs en science et technologie, il lui sera difficile de maintenir ses activités économiques et son statut mondial », déclarait Qian Xuesen, un scientifique chinois de renom ayant apporté de grandes contributions dans les domaines de l'ingénierie aérodynamique et cybernétique en Chine (Hannas *et al.*, 2013 : 4). La volonté des dirigeants chinois n'est pas uniquement d'intégrer la communauté internationale, mais plutôt de la dominer, et par le fait même, d'éviter de revivre une autre période d'humiliation face à l'Occident, comme celle vécue durant les guerres de l'Opium (1842 et 1860) (Hannas *et al.*, 2013 : 5; Pena, 2015 : 281; Poreba, 2012 : 262). Pour ce faire, elle s'est engagée depuis plusieurs décennies dans une véritable quête de technologies occidentales pour rebâtir sa grandeur et réduire son retard technologique par rapport aux puissances de l'Ouest[10].

[10] Plusieurs dirigeants chinois estiment que la technologie quantique deviendra d'ici quelques années le fer de lance de la compétitivité nationale chinoise. Depuis les révélations d'Edward Snowden en juin 2013 concernant l'étendue mondiale des capacités et des activités opérationnelles des services de renseignement américains, les programmes de recherche en matière de technologie quantique ont pris une grande ampleur. Devant ce constant, les grands pontes de l'État chinois ont démontré leur inquiétude en ce qui a trait à la sécurité de l'information, ainsi qu'aux vulnérabilités face au cyberespionnage étranger, provoquant alors la recherche de nouveaux moyens de protection conçus de manière indigène (Kania et Costello, 2018 : 6).
À titre indicatif, le New York Times rapportait le 15 juin 2020 les progrès des scientifiques chinois dans la création de ce qui semblerait être le premier relais satellitaire inviolable au monde. Utilisant la technologie quantique, la prestigieuse revue scientifique *Nature* mentionnait que le système élaboré par les Chinois produit un canal résistant aux attaques. Ainsi, en plus du lancement chinois du premier

Xi Jinping, le président actuel de la RPC, mentionnait à juste titre sa volonté ardente de faire de la Chine le chef de file mondial en S&T dans son discours prononcé au sommet du G20 en 2016. Il énonçait :

> Scientific and technological innovation holds the key to development. We are keenly aware that many sectors of China's economy are not strong or competitive enough despite their big sizes. Over the years, they have depended on input of resources, capital and labor force to achieve growth and expand scale. But this model is no longer sustainable. China now faces the challenging task of changing its growth drivers and growth model and adjusting its economic structure. To make China an innovative country and a leader in science and technology is what China must do now in pursuing development.
>
> We are implementing the innovation-driven development strategy so as to leverage the role of innovation as the primary growth driver and make growth quality based rather than quantity based. We will promote all-dimensional, multi-tiered and wide-ranging changes in principles guiding development, institutional structures and business models so as to bring about a fundamental transformation of the forces driving development and create new impetus for it. We will strive to make breakthroughs in major projects and priority areas and take the lead in undertaking major international scientific programs and projects. We will conduct research on and resolve pressing scientific and technological issues holding back economic and industrial development. We will speed up the commercialization of R&D achievements to meet the need of shifting the growth model, adjusting economic structure, building a modern industrial system, fostering strategic emerging industries and developing a modern service industry. In short, we aim to move our industries and products up to the medium-high end of the value chain and create more innovation-driven growth areas with first-mover advantages that will lead development (G20 Research Group, s.d.)

La collecte d'information sur un adversaire stratégique n'est pas un concept nouveau en Chine (Changhuo, *et al.*, 1998 : 42; Roper, 2014 : 121). Dès le 5^{e} siècle av. J.-C., Sun Tzu écrivait dans son ouvrage phare *L'Art de la guerre* :

> […] ce qu'on appelle « information préalable » ne peut pas être tiré des esprits, ni des divinités, ni de l'analogie avec des évènements passés, ni de calculs. Il

satellite quantique en 2016 (*Micius*), plusieurs spécialistes prévoient que Pékin possédera un jour son propre réseau de communication globale hypersécurisé (Broad, 2020).

> faut obtenir d'hommes qui connaissent la situation de l'ennemi (Sun Tzu, 1972 : 109)[11]

Si avec le temps, évoquer les écrits de Sun Tzu semble relever de plus en plus du cliché, la pensée stratégique de la Chine du 5e siècle av. J.-C. est pourtant encore aujourd'hui bien implantée et se positionne au cœur de la stratégie du Parti communiste chinois (PCC) (Manthorpe, 2019 : 36). En ce sens, le plaidoyer de Sun Tzu en faveur de l'utilisation du renseignement reste encore pertinent pour comprendre les pratiques employées par la Chine dans sa conquête de l'hégémonie mondiale (Manthorpe, 2019, *ibid.*).

Au fil du temps, l'espionnage chinois dans sa forme la plus archaïque s'est transformé et complexifié au gré des développements technologiques mondiaux. L'obtention d'information sur l'adversaire s'est rapidement inscrite dans une démarche économique plutôt que strictement politique et militaire. Par exemple, dès l872, les premières formes d'appétit pour les connaissances occidentales se sont manifestées sous la dynastie Qing, alors que de jeunes étudiants âgés entre 12 et 15 ans partaient étudier aux États-Unis. Ces étudiants revenaient alors en Chine mieux renseignés sur le développement de l'Occident (Hannas *et al.*, 2013 : 6). Ce genre de pratique s'est observé pendant près de 60 ans, jusqu'à ce que la Chine entre en guerre contre le Japon (1937-1945), puis a repris de façon encore plus agressive dans les années 1980 (Hannas *et al.*, 2013, *ibid.*) [12].

---

[11] Traduction libre

[12] La Chine continue aujourd'hui de surveiller le retour des étudiants diplômés à l'extérieur de ses frontières, notamment lorsqu'ils reviennent des pays occidentaux. Cette stratégie d'acquisition d'information s'observe autant par l'envoi de stagiaires dans des compagnies de secteurs jugés stratégiques. En France (2005), l'affaire impliquant l'équipementier automobile Valeo, est un cas particulièrement pertinent. Li-Li, jeune Chinoise de 22 ans originaire de Wuhan et étudiante à l'université de technologie de Compiègne (Oise), a effectué en 2005 un stage chez Valeo et a été suspectée d'avoir recopié des fichiers de l'entreprise française. Li-Li a nié jusqu'à sa remise en liberté les accusations de piratage industriel à son endroit. Elle a affirmé ne pas savoir qu'il était illégal de recopier des données informatiques pour travailler. Malgré le fait que la stagiaire ait confié aux enquêteurs français avoir copié un maximum de fichiers pour l'aider à produire son rapport de stage, les

Aujourd'hui, les Chinois sont en mesure d'imiter les pays étrangers puisqu'ils les connaissent si bien (Courmont, 2009 : 36). Barthélémy Courmont explique : « La contemplation dans l'ombre et le rejet hérité de l'ignorance ont tous deux laissé place à un plus grand pragmatisme de la part de la population qui se superpose au sentiment de fierté » (Courmont, 2009, *ibid.*). C'est donc pourquoi les dirigeants chinois sont qualifiés de pragmatiques. Leurs motivations tiennent essentiellement à deux objectifs importants : la pérennité du PCC et la montée en puissance de la Chine. Tous les moyens deviennent justifiables, du moment qu'ils permettent d'atteindre ces objectifs nationaux (Courmont, 2009 : 44). D'ailleurs, la célèbre citation de Deng Xiaoping résonne encore aujourd'hui, alors qu'elle est souvent rapportée : « peu importe la couleur du chat, tant qu'il peut attraper les souris » (Cité par Courmont, 2009, *ibid.*).

Forte de son autoritarisme et de son pragmatisme économique et géopolitique, la Chine se plaît, en l'occurrence, dans son rôle autoproclamé d'architecte du futur paysage techno-industriel. À l'aube de sa suprématie mondiale qui devrait s'être complètement réalisée en l'an 2049, au centenaire de la RPC, la Chine est pour le moins très active : elle mise de plus en plus sur la prépondérance des services de renseignement pour en connaître davantage sur l'état des autres puissances (Courmont, 2009, *ibid.*). De fait, l'Armée populaire de libération (APL), largement instrumentalisée dans le processus décisionnel en Chine, de même que le ministère de la Sécurité de l'État (MSE), le Service de renseignement extérieur chinois, sont dorénavant plus qu'enclins à repérer et instrumentaliser les nouvelles technologies des pays occidentaux dans un dessein de modernisation.

Bien que le PCC utilise également ses agences militaires et civiles de renseignement pour contrer l'espionnage étranger, là où il diffère, cependant, est dans l'accent mis sur une pluralité d'organismes officieux et de liens de personnes à personnes (*guanxi*), qui

---

enquêteurs ont trouvé dans son ordinateur, des échanges de courriels codés en provenance de Chine. Qui plus est, deux disques durs et six ordinateurs ont été trouvés à son domicile. De sérieux soupçons ont été émis par les services de renseignement français envers leur homologue chinois.

fournissent une porte d'entrée dans plusieurs pays cibles (Manthorpe, 2019 : 35). Cette offensive stratégique a été observée dans les années 1950, alors que la Chine mettait continuellement à profit un immense réseau de captation d'information qui s'est professionnalisé avec le temps. Devenue une véritable industrie de l'espionnage scientifique (Van Hoecke, 2014 : 90), la Chine de Xi Jinping harmonise les notions de créativité et de copiage (Hannas *et al.*, 2013 : 13).

2.1 L'acquisition de renseignements étrangers : une activité inhérente au processus de modernisation chinois

En Chine, l'acquisition d'information en S&T a connu une renaissance dans les années 1970. Au grand détriment des pays occidentaux, cette collecte, qui ciblait les pays les plus avancés technologiquement, a pris une grande ampleur depuis la réforme des « Quatre Modernisations » de Deng Xiaoping en 1979. Cette réforme a favorisé l'essor et le développement des secteurs de l'agriculture, de l'industrie, de la S&T et de la défense nationale. Elle portait sur une transformation économique fondamentale, permettant ultimement, par des politiques économiques d'ouverture, d'intégrer le pays dans la communauté internationale (Zheng, 2009 : 2). Celle-ci faisait en sorte que la Chine passait d'une zone de transformation des exportations à une économie mondialisée.

Cette ouverture économique sur le monde, grandement stimulée par les investissements directs étrangers (IDE), ont facilité l'intégration du pays dans la globalisation. Au début des années 1990, la Chine est devenue l'une des destinations mondiales les plus prisées en termes d'IDE. Si bien que 80 % des *Fortune 500* et les 100 meilleures compagnies de technologie dans le monde ont établi des relations d'affaires en Chine (Zheng, 2010 : 806). Dans ce nouvel élan économique, la Chine est passée d'un État-paysan à une puissance industrielle en l'espace de quelques décennies. Les IDE ont transformé

substantiellement le paysage économique chinois de telle manière que le pays est rapidement devenu la manufacture mondiale (Zheng, 2010, *ibid.*). Orientée vers l'extérieur, notamment par son caractère exportateur, la Chine s'est ainsi érigée parmi les économies les plus prospères d'Asie de l'Est (Hong Kong, Taïwan, Corée du Sud et Singapour) et du monde en très peu de temps.

C'est avec l'adoption de plusieurs programmes liés à la S&T que la Chine a acquis le statut mondial qu'elle possède aujourd'hui. Parmi ceux-ci figuraient le « Torch Program » pour la création d'industries dans le domaine de la haute technologie, le Programme 973, pour la recherche de tout genre, les programmes de réforme universitaire 985 et 211, qui visaient la création de plusieurs programmes d'études attrayants à l'intention des étudiants de retour au pays (Hannas et *al.*, 2013 : 12). De cette liste on peut y ajouter le programme des « 1000 talents », un programme de recrutement de talents étrangers qui figure parmi 200 autres programmes du même type. Or, le côté illégal de ce genre de programme s'illustre par le fait que le PCC utilise les paravents légaux de ces programmes pour obtenir des technologies étrangères clandestinement. Selon le Australian Strategic Policy Institute, ces programmes de recrutement de talents ont attiré environ 60 000 professionnels étrangers entre 2008 et 2016 (Joske, 2020). Alors que ces programmes sont attrayants pour un grand nombre de professionnels du monde entier, ils manquent considérablement de transparence, car ils sont notamment associés au vol de propriété intellectuelle pour contribuer à la modernisation de l'APL (Joske, 2020).

Or, le programme lié à la S&T le plus connu est sans doute le Programme 863 lancé en 1986. Ce programme, créé pour faire face aux nouveaux défis globaux qu'engendrent la compétition internationale, se focalisait sur la biologie, l'aérospatial, les télécommunications, le laser, l'automatisation, l'énergie, les nouveaux matériaux et l'océanographie (Hannas *et al.*, 2013, *ibid*.). Coordonné à l'époque par le PCC, le Programme 863 avait un mode opératoire rassemblant des tactiques d'acquisition légales et illégales de renseignements scientifiques et techniques aux États-Unis

(Burstein, 2009 : 969-970)[13]. Il visait l'intensification des efforts en matière d'innovation scientifique et technologique, afin d'accélérer le développement de la Chine dans le secteur de la haute technologie (Roper, 2014 : 43). Précisément, le Programme 863 a mobilisé 3000 scientifiques pour atteindre en 10 ans 1500 objectifs dans les domaines de l'économie et de la défense (Faligot, 2019 : 250-251). Ce programme a bénéficié de la politique des « 16 caractères » décrétée par Deng Xiaoping en 1978, qui faisait mention de la nécessité de jumeler les domaines civil et militaire dans le but d'effacer les frontières entre les opérations d'États et les activités commerciales (Faligot, 2019 : 251). Dans ce contexte, les scientifiques les plus notoires et expérimentés de l'époque ont été choisis pour réduire l'écart entre les pays occidentaux et la Chine en matière de défense avancée, d'aéronautique, de technologies spatiales, de technologies de l'information, de lasers, d'automatisation, d'énergie et de nouveaux matériaux (Faligot, 2019, *ibid.*). En ce qui a trait aux secteurs liés au renseignement militaire, le Programme 863 se focalisait sur les éléments suivants (Faligot, 2019, *ibid.*) :

- Guerre biologique (recherches sur les gènes et les mutations génétiques)
- Technologies spatiales (notamment les satellites de reconnaissance [satellites espion])
- Technologies de l'information (en particulier l'intelligence artificielle, l'informatique, l'interception d'images, permettant le développement des systèmes 3CI « Command, Control, Communications & Intelligence », afin de créer des logiciels pour des applications militaires)
- Armes au laser (technologie plasma et spectroscopie)
- Robotique (armes intelligentes et robots-soldats)
- Armes nucléaires (réacteurs refroidis au gaz)
- Matériaux « exotiques » (métaux rares, matières composites, etc.)

[13] Les rapports du Congrès des États-Unis indiquaient que l'objectif du Programme 863 consistait à rétrécir l'écart scientifique et technologique entre la Chine et l'Occident pour l'an 2000. (Burstein, 2009, p. 970)

En 2006, une certaine intensification, ou du moins, un nouvel élan s'est produit concernant l'acquisition de renseignements étrangers. Le ministre des Sciences et Technologies de l'époque, Xu Guanghua, constatait que 70 % des brevets exploités en sol chinois ne provenaient pas du pays. Le concept d'« innovation indigène » s'est alors retrouvé dans un plan étalé sur 15 ans, et le *PRC Medium and Long-Term S&T Plan* a été créé (Van Hoecke, 2013, p. 33). Ce plan avait pour but de permettre à la Chine d'inverser cette tendance pour l'année 2020, alors que 70 % des brevets deviendraient originaires de la Chine. Cependant, si le concept d'innovation indigène saisit bien le renversement de tendance des politiques économiques, le concept de « réinnovation » est beaucoup plus évocateur quant au mode opératoire. Van Hoecke définit la réinnovation comme une stratégie « d'importation, d'absorption et d'assimilation du savoir-faire étranger » (Van Hoecke, 2013, p. 32). Concrètement, elle explique :

> C'est la méthode que la Chine a choisie en 2006 pour rattraper son retard industriel : elle va déposer des brevets chinois, indigènes, sur les technologies étrangères. […] Les dépôts de brevets « domestiques » ont été multipliés par trois entre 2005 et 2010. On peut espérer que les ingénieurs et chercheurs chinois apporteront de petites améliorations aux brevets étrangers « réinnovés ». […] La réinnovation est la pierre angulaire de la stratégie chinoise de développement industriel par l'innovation[14] (Van Hoecke, 2013, *ibid.*)

Le concept d'« innovation indigène » ou « innovation nationale » est un élément fondamental de la politique de développement économique de la Chine depuis les années 2000. Celui-ci consiste à transformer le modèle de la croissance économique, passant d'une économie basée sur les ressources naturelles et de la main-d'œuvre à une économie qui bénéficie de l'innovation technologique (Jingxia, 2010).

[14] En pratique, le concept de réinnovation n'illustre pas des activités qui ont émergé en 2006. L'un des exemples les plus frappants à ce sujet est sans doute l'appel d'offres lancé par la Chine en 2004 pour développer son réseau ferroviaire. Pendant que la Chine faisait monter les enchères et laissait entrevoir des contrats onéreux, les compagnies Siemens, Bombardier et Mitsubishi ont procédé consciemment à d'importants transferts de technologie pour la construction de trains à grande vitesse. Selon Arnaud Aymé, associé au cabinet de conseil Sia Partners : « Il n'a fallu qu'un peu moins de 10 ans pour voir les groupes locaux maîtriser les technologies et candidater à l'export » (Lamigeon, 2013).

Jumelée au plan de renouvellement stratégique chinois en S&T, la loi chinoise sur la sécurité nationale de 2015 réitère, par ses articles 3 et 8, l'importance prépondérante d'une union entre sécurité nationale et développement économique (Ministère de la Défense de la République populaire de Chine, 2017). L'article 3 souligne que la sécurité nationale doit adhérer à une perspective plus globale, laquelle doit porter un regard sur l'élément fondamental de la sécurité du pays, soit la sécurité économique. L'article 8 prescrit, pour sa part, que la sécurité nationale doit être maintenue en fonction du développement économique et social (Ministère de la Défense de la République populaire de Chine, 2017).

2.1.1 L'intelligence économique chinoise en pratique

En Chine, la quasi-totalité des entreprises est intimement liée au PCC (ARTE, 2016), de sorte que les ambitions d'une compagnie et les intérêts nationaux ne font sensiblement plus qu'un. Or, à l'instar du Japon durant la dernière moitié du 20^{e} siècle, la Chine est consciente que l'intelligence économique est un outil incontournable pour protéger la propriété intellectuelle et pour atteindre le statut de superpuissance économique (Slate, 2009 : 7). Au milieu des années 1990, de nombreux étudiants chinois se sont focalisés sur l'intelligence économique et l'utilisation du renseignement au service des intérêts nationaux (Slate, 2009, *ibid.*). Au fil des ans, certains de ces chercheurs sont devenus des individus influents dans le secteur privé et le secteur public, en occupant, par exemple, des postes de direction, soit dans des firmes de consultation, soit dans des services gouvernementaux (Slate, 2009, *ibid.*).

En Chine, l'intelligence économique est une pratique relativement nouvelle, qui a émergé avec les réformes économiques des années 1970 (Changhuo *et al.*, 1998 : 42). Elle est devenue un concept pratique central dans l'économie nationale chinoise ainsi que dans le développement des entreprises (Changhuo, *et al.*, 1998, *ibid.*). En 1984, la

Sichuan Scientific and Technical Information Center (SSTIC) a été fondée, et impliquait, à l'occasion, la création du réseau d'information FAX, un réseau de partage d'information stratégique relative aux renseignements commerciaux (Faligot, 2019 : 277). Le SSTIC comptait également à l'époque sur un service dédié à la collecte et l'approvisionnement d'échantillons de produits étrangers (Faligot, 2019, *ibid.*).

Durant la même période, le ministère chinois des Relations et du Commerce de l'économie étrangère (MOFTEC) était considéré comme le véritable moteur derrière l'établissement du réseau économique chinois, qui unifiait les entreprises locales et régionales, ainsi que celles du secteur de l'import-export (Faligot, 2019, *ibid.*). Roger Faligot précise, dans son ouvrage *Chinese Spies*, que ce réseau de partage de l'information bénéficiait d'un terminal satellite et d'un réseau électronique d'échange de données. Grâce à ce système comparable au système japonais, la Chine prévoyait, sur une durée de cinq ans, construire 300 stations terrestres pouvant acheminer simultanément des données économiques vers la base de données centrale à Pékin, ainsi que vers les entreprises, facilitant dans un même temps, l'intervention des entreprises à l'étranger (Faligot, 2019, *ibid.*).

En Chine, une myriade de services gouvernementaux est, depuis la seconde moitié du 20^{e} siècle, au service de la surveillance économique et de la recherche de renseignements de tout genre (Faligot, 2019 : 405). Pour n'en nommer que quelques-uns : le Research Bureau, le ministère du Commerce (MOFCOM) (en remplacement du MOFTEC) et le ministère des Sciences et Technologies (MOST). Dans le cas du MOFCOM, Roger Faligot souligne que sa division du renseignement, qui a été élargie après 2003, avait pour mission de reproduire la même transformation nationale en matière économique, qui a eu lieu quelques années avant, mais à l'échelle mondiale. Que ce soit pour occuper une position importante au sein de l'Organisation mondiale du commerce (OMC), négocier des traités relatifs à la propriété intellectuelle, définir des axes de stratégies commerciales ou créer des coentreprises (*joint ventures*), la

Chine devait impérativement mettre sur pied des techniques de partage et bâtir une expertise en intelligence économique (Faligot, 2019 : 280-281).

En théorie, tant du côté chinois qu'américain, l'intelligence économique devant reposer sur des pratiques légales et éthiques, fait l'unanimité. Or, les deux côtés admettent qu'il existe une zone grise en la matière, où l'ingénierie inversée ou la rétrotechnique (*reverse engineering*[15]) et le transfert de propriété intellectuelle ont lieu sans nécessairement enfreindre la loi, et où l'intérêt public peut prévaloir sur la considération éthique (Slate, 2009 : 8). Les deux parties conviennent également que des pratiques comme la surveillance téléphonique, les communications Internet ainsi que le vol de secrets commerciaux sont défendues. Cependant, comme l'indique Robert Slate, la réalité démontre que la pratique diffère substantiellement de la théorie (Slate, 2009 : 8). En effet, plusieurs cas montrent qu'au contraire, un grand nombre de compagnies chinoises utilisent de plus en plus leurs unités internes de renseignement pour améliorer l'efficacité de leurs activités illégales (Slate, 2009, *ibid.*). Tel serait d'ailleurs le cas avec Huawei, le géant des télécommunications chinoises, qui est soutenu par un système d'intelligence économique (Huawei TopEng-BI) questionnable à plusieurs égards (Faligot, 2019 : 286)[16]. Ce système, écrit Roger Faligot :

> […] depends on the internal and external flow of information and information liaison with all its subsidiairies and the following network: a real-time data warehouse, an online analysis process, data-mining, an AI system, and geographical information system. The complexe interface of these sectors gives access from Huawei's massive headquarters in Shenzhen to analyses, information and market projections, an effective sales support, and detailed

[15] L'ingénierie inversée ou la « rétro-ingénierie » est un processus qui vise à décortiquer une technologie, un objet ou un matériau pour en connaître ultimement son fonctionnement interne, ainsi que chaque étape de sa fabrication.

[16] L'entreprise Huawei a été dirigée jusqu'en 2018 par Sun Yafang, ingénieure de formation et ancienne technicienne de premier plan à la division des télécommunications au MSE. D'ailleurs, selon un rapport de la RAND Corporation de 2005 rédigé par Evan S. Meideros, Roger Cliff, Keith Crane et James C. Mulvenon, destiné à la US Air Force, Huawei maintient de profondes relations avec l'appareil militaire chinois, lequel joue un rôle multidimensionnel, aussi bien en tant que client important que partenaire en R&D (Cité par Hamilton, 2018 : 156).

> analyses of the company's clientele, which presumably also enables access to vast amounts of personal data (Faligot, 2019, *ibid.*)

Ces unités internes de renseignement se retrouvent souvent à l'extérieur des frontières de la Chine, dans des centres de R&D, et accomplissent un travail depuis ce qui est communément appelé des « postes d'écoute » (*listening posts*) (Slate, 2009, *ibid.*). Ces postes de surveillance, comme l'explique Robert Slate, permettent une collecte d'information plus efficace sur les concurrents et, simultanément, une analyse de la propriété intellectuelle, de la littérature technique, des brevets, des produits d'échantillon, etc. (Hannas *et al.*, 2013 : 44).

Or, bien qu'il subsiste certaines similitudes entre la Chine et les pays occidentaux en matière d'intelligence économique, plusieurs différences s'observent. L'une d'entre elles réside dans le fait que la Chine combine le personnel civil (ingénieurs, scientifiques, techniciens) au personnel du renseignement et de l'appareil militaire (Slate, 2009 : 9; Faligot, 2019 : 254, 279; Meia Nouwens et Helena Legarda, 2018). Ainsi, afin de mettre sur pied un processus de collecte efficace (de l'acquisition de l'information à sa dissémination), le personnel civil travaille conjointement avec les services de renseignement en leur fournissant notamment de l'information sur les analyses de brevets et les études de marché (Slate, 2009, *ibid.*). Dans bien des cas, ces postes d'écoute reçoivent un soutien financier de la part des services de renseignement ou de l'appareil militaire, pour mener des activités clandestines comme le piratage informatique (Slate, 2009, *ibid.*).

En Chine, plusieurs chefs d'entreprise ont des visées mondiales (Slate, 2009 : 2, 8, 13). L'intelligence économique est, en ce sens, l'outil nécessaire pour améliorer leur gestion stratégique, ainsi que pour repérer les firmes étrangères susceptibles d'être achetées. Cette ambition, largement répandue dans le monde entrepreneurial chinois, crée un terreau fertile pour des pratiques de renseignement illégales (Slate, 2009, *ibid.*). Des pratiques illégales comme la collecte de renseignements HUMINT et SIGINT, sont

comprises dans des programmes d'intelligence économique dédiés aux entreprises soutenues par le PCC (Slate, 2009 : 2). Cette propension chinoise aux activités illégales témoigne d'ailleurs d'une approche stratégique et pragmatique qui montre explicitement l'évolution des premières conceptions chinoises de l'autosuffisance (Hannas *et al.*, 2013 : 13). Celles-ci sont représentées dans le concept de « *ti-yong* », qui exprime la conservation des fondements et de l'essence de la société chinoise, et ce, en comptant sur la technologie occidentale pour atteindre certains objectifs stratégiques (Hannas *et al.*, 2013, ibid.). De plus, et à la grande différence de ce qu'on observe chez les Occidentaux, plusieurs entreprises chinoises investissent non seulement des ressources dans l'intelligence économique, mais également dans le contre-espionnage (Slate, 2009 : 8). La Chine considère que les efforts consentis pour acquérir de l'information doivent être protégés, de sorte que la notion de propriété s'applique tant aux activités qu'aux produits, peu importe si les activités sont légales ou non (Slate, 2009 : 8). En l'occurrence, les programmes de contre-espionnage entrepreneuriaux permettent de protéger ce qui a été acquis par les programmes offensifs d'intelligence économique.

2.1.2 Le renseignement chinois : du mythe à la réalité

À la lumière de l'imbrication de la communauté du renseignement et des professionnels scientifiques en Chine, l'acquisition de la propriété intellectuelle et les diverses activités de collecte sont perçues comme des enjeux de sécurité nationale. En Chine, la frontière qui sépare les services de renseignement du monde corporatif est excessivement poreuse, et lève conséquemment le voile sur l'influence et le contrôle du gouvernement en matière d'intelligence économique (Slate, 2009 : 11). Cette dynamique illustre, par ailleurs, l'étendue du réseau chinois : un réseau composé d'un grand nombre d'individus, dont le degré de contribution des principaux services de renseignement varie selon les objectifs (Faligot, 2019 : 252). En effet, dans certains

cas, tant sur le plan des opérations que de la coordination, les activités clandestines ne sont pas toujours imprégnées des agences de renseignement les plus notoires (comme le MSE, l'APL ou le Bureau de la Sécurité d'État à Shanghai [SSB]), mais également d'autres agences subordonnées aux directives du PCC (Mattis, 2012 : 679, cité dans le *Cox Report*, 1999 : 52-53; Roper, 2014 : 57, 91; Poreba, 2012 : 263). Parmi ces agences se trouvent le ministère de la Sécurité publique, qui est la principale autorité policière (MSP), le Second Département de l'Armée populaire de Chine (GSD ou 2PLA) et le Bureau de liaison du Département des politiques générales (GPD), subordonné au Département des politiques générales de l'APL (Mattis, 2012, *ibid.*).

Toutefois, l'exploitation de ce réseau d'individus doit être nuancée et éloignée du raccourci simpliste très répandu que suppose la théorie du « grain de sable » ou *thousand grains of sand*, *human-wave* ou *mosaic* pour définir le mode opératoire des services de renseignement chinois. Cette théorie, illustrée par des exemples fictifs, se lit comme suit :

> Si la composition du sable sur une plage était considérée comme une cible du renseignement par les nations du monde, certains pays relèveraient le défi en envoyant un sous-marin au large de la plage. Dans l'obscurité de la nuit, une équipe de commandos sortirait du sous-marin, pagayerait dans un radeau jusqu'à la plage, ramasserait un seau ou deux de sable pour en récolter une bonne quantité de données. D'autres pays feraient usage de leurs satellites, afin de bénéficier de *scanners* infrarouges et spectrographiques au phosphore. […] La Chine, quant à elle, demanderait à dix mille de ses citoyens de passer une journée à la plage. Au coucher du soleil, ces derniers retourneraient tous chez eux pour y secouer leurs serviettes; et les Chinois auraient plus de sable et plus de données que les autres nations (Moore, 1997, cité par Hannas, *et al.*, 2013 : 189)[17]

Largement critiquée par plusieurs spécialistes de la question (Moore, 1997, Mattis, 2012; Hannas, *et al.*, 2013), la théorie du grain de sable suppose que les services de renseignement chinois dépendent étroitement d'une collecte effectuée par des amateurs

[17] Traduction libre

(Mattis, 2012 : 680). Selon Peter Mattis : « la définition même d'une bureaucratie permanente du renseignement suppose le professionnalisme, même si la performance n'est pas à la hauteur d'une norme arbitraire » (Mattis, 2012 : 681). En effet, considérer la théorie du grain de sable revient à concevoir le renseignement chinois comme des services qui sont dans l'incapacité de combler les besoins de Pékin en matière de renseignement (Mattis, 2012, *ibid.*). De plus, soutenir cette théorie sous-tend la croyance selon laquelle les services chinois ne collectent pas d'informations avec une intention délibérée (Mattis, 2012, *ibid.*).

Plusieurs cas montrent en effet le contraire, et prouvent que la collecte d'information est une activité qui illustre plus souvent qu'autrement, un lien direct entre l'expertise, les besoins et les tâches assignées (Hannas *et al.*, 2013 : 190). Dans le cas particulier de Chi Mak, un ingénieur américain d'origine chinoise reconnu coupable en 2007 de complot en vue d'exporter des technologies de défense en Chine, il est évident que les renseignements transmis étaient ciblés et que l'opération était préméditée. En effet, deux documents incriminants ont été retrouvés chez lui. Le premier, rédigé en mandarin le pressant de joindre des associations professionnelles et d'assister à davantage de séminaires sur des questions de recherches avancées, et le deuxième, une liste de technologies précises, comme les torpilles, les systèmes électroniques de porte-avions, la propulsion sous-marine et les plateformes de lévitation magnétique pour les lancements spatiaux (Hannas *et al.*, 2013 : 190-191).

De surcroît, Paul Moore, ancien directeur du contre-espionnage chinois au FBI, soulignait deux ans après la sortie du Rapport Cox en 1999 : « […] les individus qui collectent du renseignement pour la Chine, ne ressemblent généralement pas à des espions, n'agissent pas comme des espions et ne dérobent pas nécessairement de grandes quantités de renseignements à la fois (Faligot, 2019 : 253). Selon lui, comme le reprend Roger Faligot, dans la plupart des cas, le travail de veille et de collecte de données, autant « sensibles » qu'elles peuvent l'être, est réalisé par des chercheurs universitaires, des étudiants, des gens d'affaires, des scientifiques ou des journalistes,

par l'entremise de relations professionnelles ou amicales (Faligot, 2019 : 253; Katsuya et de Pierrebourg, 2010 : 237). Qui plus est, la Chine mise sur un réseau réunissant des officiers du renseignement et des individus cooptés basés en Chine (Mattis, 2012 : 692). La plupart des activités de collecte clandestines aux États-Unis, par exemple, sont effectuées par des individus rattachés au PCC ou à des entreprises qui ne sont pas affiliées aux services de renseignement officiels (Roper, 2014 : 50). Ces individus recueillent de leur côté des renseignements concernant certaines technologies, sans nécessairement compter sur l'appui des agences de renseignement chinois (Roper, 2014 : 57). En somme, cette approche « par couches » (*layered approach*) permet, en outre, de mobiliser et d'unir les services d'État et la société civile dans le but de servir l'intérêt national.

En tout état de cause, il existe autant de différences que de similitudes entre les pratiques de renseignement occidentales et chinoises. En effet, les méthodes opérationnelles et les objectifs liés à la collecte de renseignements ne diffèrent pas autant que certaines analyses pourraient le prétendre. En revanche, des différences persistent dans ce domaine, notamment en ce qui a trait aux traditions sociales et intellectuelles (Mattis, 2012 : 693). Les méthodes du renseignement chinois demeurent somme toute difficiles à appréhender pour les Occidentaux. Ce faisant, deux éléments fondamentaux demeurent sous-explorés dans la littérature, selon Peter Mattis. Le premier concerne les relations interpersonnelles chinoises, précisément la façon dont les officiers du renseignement chinois adaptent leur approche de recrutement à l'égard des Occidentaux. Le deuxième concerne les différences méthodologiques occidentales et asiatiques à l'égard des modes d'analyse. En Occident, la logique fonctionne à travers une structure d'analyse plus formelle, afin de résoudre des problèmes de façon systémique, alors qu'en Asie de l'Est, la logique témoigne davantage d'une approche relationnelle et holistique (Mattis, 2012, *ibid.*).

2.1.3 Au-delà de l'espionnage : la gestion de l'information et l'acquisition de l'OSINT en matière de S&T

Comme nous venons de le voir, l'acquisition d'information sur les technologies étrangères par la Chine se fait par de nombreuses factions, organisations et individus. Cette observation ne distingue toutefois pas pour autant la Chine de ses concurrents. Se servir d'un réseau qui va au-delà du personnel du renseignement n'est pas révolutionnaire en soi; plusieurs pays ont recours à cette stratégie pour acquérir de l'information au moyen de sources ouvertes. Par exemple, de nombreuses nations ont, par le passé, utilisé leur communauté émigrée pour accaparer des secrets à l'étranger (Poreba, 2012 : 260). Ce qui différencie également la Chine des autres nations est sa conception de la gestion de l'information en matière de S&T. Dès le début des années 1990, le processus d'acquisition d'information de type OSIF a été réorganisé en Chine, de sorte que les objectifs, les cibles et la méthodologie ont également connu des évolutions majeures (Hannas *et al.*, 2013 : 25).

L'ouvrage notoire *Sources and Methods of Obtaining National Defense Science and Technology Intelligence* (écrit en 1991 par Huo Zhongwen et Wang Zongxiao, deux ex-espions) surnommé par plusieurs, et peut-être exagérément selon certains, le *China's Spy Guide* ou *China Spy Manual*, prétend essentiellement que la densité et la variété de l'information en matière de S&T requiert un véritable changement méthodologique qui permettrait de reconcevoir les activités de collecte pour être en mesure d'optimiser la gestion de l'information acquise (Hannas *et al.*, 2013 : 26)[18]. Selon les auteurs, les techniques de collecte plus traditionnelles sont incompatibles

[18] Carl Roper ajoute dans son ouvrage *Trade Secret Theft, Industrial Espionage and the China Threat* : « What makes the manual exceptionally interesting is that any country could use it to target the United States for the purposes of attempting to gain the desired information, that is, not just China, but virtually every country that wishes to target the United States, if desired. Also, any country could use the manual as a blueprint for revisiting it and creating a specific manual against any other country. […] The United is the most open nation in the world. The manual was developed based upon that simple fact. No other nation allows such openness in terms of access to government, private industry, think tanks, developing technologies, and the like » (Roper, 2014 : 91)

avec l'incalculable masse de données générées à l'étranger (Hannas *et al.*, 2013, *ibid.*). Brièvement, les anciennes pratiques comprenaient : 1) la collecte de données et l'attente de l'utilisation des clients; 2) l'appréciation de la quantité d'information collectée; 3) la focalisation sur les documents uniquement écrits; 4) la considération isolée de sa propre collecte d'information; 5) l'embauche de personnel dont le seul atout est la connaissance d'une langue étrangère; et 6) le déboursement sans planification (Hannas *et al.*, 2013, *ibid.*). Le nouveau paradigme que Huo et Wang ont mis de l'avant au début des années 1990 impliquait : 1) la collecte ciblée; 2) la collecte de divers types de média et la création de bases de données; 3) la perception de la collecte comme une science appuyée sur une théorie des systèmes; 4) l'embauche d'experts en technologies de l'information; et 5) la planification avant le déboursement (Hannas *et al.*, 2013, *ibid.*).

L'acquisition de l'OSIF fait ainsi l'objet d'une véritable professionnalisation en Chine (Hannas *et al.*, 2013 : 44). Pour ainsi dire, la Chine, plus que n'importe quelle autre nation, collecte de l'information par ce type de sources (Roper, 2014 : 95). Contrairement aux pays occidentaux où l'OSIF en matière de S&T sert généralement à garder un œil sur les développements des nations adverses, la Chine quant à elle, conçoit l'acquisition d'information étrangère dans un effort offensif et méthodique pour accélérer son développement scientifique (Hannas *et al.*, 2013, *ibid.*). Car l'utilisation de l'OSIF est peu coûteuse, légale et sert de complément à l'information classifiée obtenue. De plus, la transformation de l'information brute étrangère en renseignement utile profite tout autant à diminuer, voire à « contourner le coût et les risques associés à la recherche indigène » (Hannas *et al.*, 2013, *ibid.*).

Cependant, comme le soulignent William Hannas, James Mulvenon et Anna Puglisi, une énorme différence subsiste entre ce qui est nécessaire pour surveiller ouvertement les programmes techniques étrangers et l'appareil nécessaire pour modéliser secrètement les processus de R&D étrangers. La Chine investit une grande somme dans la collecte d'information ouverte, et ce, bien plus que d'autres pays. Ainsi, les analyses,

les interactions avec les clients et les rétroactions avec les « collecteurs » jouent un rôle de premier plan (Hannas *et al.*, 2013, *ibid.*). En l'occurrence, les auteurs ajoutent :

> […] western services typically regard open-source as a poor cousin to "real" (clandestine or technical) intelligence, China staffs its OSINT organizations with top-line career personnel, backed by an industrial organization with its own trade journals. We know of no other nation where open-course intelligence enjoys this level of support (Hannas *et al.*, 2013, *ibid.*)

Les auteurs poursuivent en mettant en lumière l'existence de la société d'État China Society for Scientific and Technical Information (CSSTI), une ONG prétendue sans but lucratif créée en 1964 dont l'objectif de base consiste encore aujourd'hui à faciliter le transfert de technologies étrangères (Hannas *et al.*, 2013 : 45). Les auteurs précisent :

> CSSTI's task are to promote open-source intelligence research, provide consulting and other services "to meet various information requirements for the nation," strengthen links between the S&T intelligence network's central and local units and between the organizations and their individual members, and acknowledge outstanding personal achievements in S&T intelligence – in essence to create a "home" for China's S&T information workers. […] CSSTI also manages the Society of Competitive Intelligence of China, one of its 11 disciplinary committees. SCIC claims 400 corporate and more than 80 individual members from among "China's 20,000-plus intelligence research and information consulting personnel." (Hannas *et al.*, 2013 : 44-45)

Ceci étant dit, lorsqu'il est question d'acquisition d'information dans le contexte chinois, il est important de souligner la qualité interchangeable des termes *information* (*xinxi*) et renseignement (*qíngbào).* Si nous avons expliqué la différence entre les deux termes au premier chapitre, cette distinction témoigne en revanche d'une conception occidentale. En Chine, ce qui relève de l'information et du renseignement ne repose pas sur des différences aussi marquées. Comme l'expliquent les auteurs de l'ouvrage phare *Chinese Industrial Espionage,* le mot *qíngbào* désigne plusieurs termes, de sorte qu'il englobe, jusqu'à une certaine mesure, tant le renseignement que l'information. Traduit préalablement du mot *information* en russe, le *qíngbào* désignait

en Chine jusqu'aux années 1970, tant la collecte clandestine que l'acquisition de sources ouvertes (Hannas *et al.*, 2013 : 46). Encore aujourd'hui, la distinction n'est pas aussi nette et reste nébuleuse à plusieurs égards, selon la personne qui exploite l'information, pour qui, et pour quelle raison. Pour une firme étrangère qui possède des laboratoires de recherche en Chine, et qui fait affaire avec le PCC, il est excessivement difficile de savoir si l'information partagée sert la communauté scientifique chinoise ou les services de renseignement chinois (Hannas *et al.*, 2013 : 47).

2.2. Le réseau du PCC et ses ambitions militaires

À maintes reprises, Xi Jinping soutient dans ses discours la création d'une économie dont le moteur est l'innovation. C'est d'ailleurs à ce titre que ce dernier prône l'idée de faire de la Chine un leader global dans les domaines scientifique et technologique d'ici 2035 (Jing, 2018). Cette approche fait écho au mantra chinois, le « rêve chinois », calqué du concept américain *the American Dream*. Ce slogan a été lancé par Xi Jinping dans les années 2010, encourageant le renforcement du patriotisme par les valeurs confucéennes, dans le but de rebâtir la gloire de l'Empire du Milieu. Cependant, faire de la Chine un modèle mondial en S&T ainsi qu'en termes d'épanouissement social, reste un idéal qui se confronte à celui des États-Unis. Les deux grands modèles se différencient grandement à plusieurs titres, notamment dans la manière dont l'économie doit être stimulée et orientée. Aux États-Unis, comme dans tous les pays occidentaux, ce sont les principes libéraux de la « main invisible du marché » qui dictent le développement de l'économie, alors que les forces naturelles réglementent le marché libre. *A contrario*, la Chine prêche plutôt pour une planification de l'économie dans laquelle son développement est soumis aux interventions de l'État.

La Chine devient néanmoins un adversaire de taille pour plusieurs États, particulièrement depuis qu'elle est soutenue par un large éventail de politiques

industrielles, contenues dans le projet de 2015, appelé « *Made in China 2025* » (MIC25) (Jing, 2018). Ce projet est, selon Scott Kennedy du Center for Strategic and International Studies (CSIS), largement inspiré du modèle de développement industriel allemand « *Industrie 4.0* », visant pour l'essentiel la réorganisation des moyens de production par l'application de la technologie de l'information (Kennedy, 2015). Focalisé sur l'idée d'être plus compétitive que les États-Unis dans les industries stratégiques, le gouvernement chinois joue un grand rôle dans l'instauration d'un cadre économique global, particulièrement en utilisant des moyens fiscaux et en soutenant des centres d'innovation dans le secteur manufacturier, l'objectif étant d'en soutenir 40 d'ici 2025 (Kennedy, 2015). Le plan économique MIC25 prévoit également un solide appui à l'égard des institutions de marché, un renforcement marqué par la protection des droits de propriété intellectuelle, tant pour les petites que les moyennes entreprises (PME), ainsi que par l'utilisation plus efficace de la propriété intellectuelle dans la stratégie commerciale (Kennedy, 2015).

Précisément, le PCC coordonne de façon centralisée la mise en œuvre du MIC25, ainsi que les politiques industrielles connexes (Zenglein et Holzmann, 2019 : 11). Contrairement au plan de politiques économiques nationales du *PRC Medium and Long-Term S&T Plan* (2006), le MIC25 préconise davantage une approche bénéfique pour les entreprises privées, l'entrepreneuriat et les mécanismes de marché, tout en améliorant la compétitivité des sociétés d'État, considérées comme incontournables dans l'entreprise de modernisation chinoise (Zenglein et Holzmann, 2019, *ibid.*). Parmi ces entreprises se trouvent : Huawei (privé), ZTE (État), Sense Time (privé), Commercial Aircraft Corporation of China (État), China Shipbuilding Industry Corporation (État), China Railway Construction Corporation (État), Alibaba (privé), Hanergy (privé), Yito Group (État), Shanghai Phichem (privé), Jiangsu Hengrui Medicine (privé), etc. (Zenglein et Holzmann, 2019 : 70, 71, 72).

Cependant, même si la Chine rêve de grandeur, la réalité démontre qu'elle continue de dépendre fortement des produits étrangers de haute technologie : une dépendance qui

freine en l'occurrence les ambitions nationales de Pékin. Comme l'avance le rapport du Mercator Institute for China Studies (MERICS) :

> Even though the country is particularly strong in the application of future technologies, its dependence on foreign high-tech products remains a major bottleneck for national tech ambitions. The most advanced components and machinery still need to be imported. Adjusted for computers and telecommunication equipment, China's reliance on foreign technology results in a negative trade balance, according to the Chinese National Bureau of Statistics' (NBS) own definition of high tech, which includes the high-end spectrum of biotechnology, life science and technology, opto-electronics, electronics, computer-integrated machinery, and aerospace (Zenglein et Holzmann, 2019 : 24)

Afin de pallier les faiblesses de la Chine, le PCC continue d'appuyer les efforts de collecte d'information à l'étranger. Concrètement, il s'appuie sur un réseau mondial de captation d'information technologique, lequel renferme des organisations politiques et non politiques (Hannas *et al.*, 2013 : 105).

2.2.1 Le réseau extérieur chinois

La conception chinoise de l'intelligence ne reflète pas seulement la volonté d'améliorer l'efficacité et l'efficience des stratégies informationnelles, comme la veille stratégique, la gestion des connaissances et la protection de l'information. L'intelligence économique de la Chine témoigne aussi d'une stratégie-réseau dont l'amplitude se mesure à l'échelle mondiale (Hannas, 2013, *ibid.*). En matière de transfert de technologie, la Chine mise sur une myriade d'organisations dont les liens avec le PCC et les impératifs technologiques diffèrent sensiblement. Néanmoins, toutes ont pour objet commun l'acheminement d'information vers Pékin. Ce faisant, puisque les États-Unis sont la cible principale des activités d'espionnage chinois, nous consacrerons cette partie sur deux réseaux chinois de transfert de technologie basés aux États-Unis.

Comme le montrent Hannas, Mulvenon et Puglisi, cinq types d'organisations chinoises composent essentiellement les canaux par lesquels la Chine collecte de l'information stratégique : les bureaux diplomatiques, les sociétés de facilitation, les ONG, les organisations culturelles (Instituts Confucius) et les associations d'anciens étudiants/réseau universitaire (Hannas, 2013, *ibid.*). Voici les deux principaux canaux intimement interreliés : le réseau diplomatique et le réseau universitaire.

Le réseau diplomatique

Au sommet de l'administration du PCC, les directives relatives aux programmes dédiés à l'influence sont formulées par le Politburo (Bureau politique) et acheminées au Comité central du PCC. Les responsabilités se divisent alors entre deux services : l'Overseas Chinese Affairs Office et la United Front Work Department. Les fonctions et les rôles, pour autant différents qu'ils soient, sont par la suite canalisés et coordonnés par les ambassades et les consulats (Hamilton, 2018 : 177). Par l'entremise de toutes les missions diplomatiques chinoises aux États-Unis (y compris celles de l'ONU et les missions consulaires), réalisées dans tout le pays (Washington D.C., New York, Chicago, Houston, San Francisco et Los Angeles), chaque bureau possède de nombreux fonctionnaires de l'État spécialisés dans le domaine de la S&T, afin de fournir un soutien aux transactions économiques réalisées entre les deux pays (Hannas *et al.*, 2013, *ibid.*)[19]. Cependant, les missions diplomatiques chinoises aux États-Unis sont particulièrement animées par un objectif précis : le transfert de technologies (Hannas *et al.*, 2013 : 106). Cet objectif se manifeste explicitement lorsque la Chine favorise la promotion de ses relations d'affaires avec les États-Unis en matière de

[19] En raison de soupçons d'espionnage économique liés à la fabrication d'un vaccin contre la COVID-19, l'administration Trump a ordonné en juillet 2020 la fermeture complète du consulat chinois de Houston. Selon des images filmées, des individus à l'intérieur de l'enceinte du consulat ont été aperçus en train de brûler des documents avant de devoir quitter l'établissement.

technologie, et implicitement, lorsqu'elle tire parti de ses relations grâce à des groupes d'intérêt chinois basés aux États-Unis (Hannas *et al.*, 2013, *ibid.*)[20].

Le réseau diplomatique chinois assure également l'anonymat du service de renseignement chinois, surtout des officiers du renseignement militaire de l'APL. D'ailleurs, comme l'affirme Carl Roper à juste titre, les agences de renseignement de la RPC opèrent aux États-Unis par l'entremise d'entreprises commerciales, en utilisant l'environnement des affaires comme couverture (Roper, 2014 : 57). Par ailleurs, les officiers du renseignement de l'APL profitent souvent d'une couverture d'attachés militaires à l'ambassade de Washington D.C., ainsi qu'à l'ONU à New York (Roper, 2014, *ibid.*).

Au quotidien, plusieurs représentants de l'ambassade de la RPC et des bureaux consulaires rencontrent les membres des groupes d'intérêt basés aux États-Unis pour communiquer les décisions politiques, demander un quelconque soutien politique, ainsi que pour informer les membres concernant les possibilités d'investissement en matière de S&T (Hannas *et al.*, 2013, *ibid.*). De la même manière, les représentants de l'ambassade chinoise aux États-Unis vont favoriser le processus administratif pour les individus qui souhaitent s'établir en Chine, pour ensuite les surveiller et veiller à ce qu'ils rencontrent les personnes clés (Hannas *et al.*, 2013, *ibid.*). De façon générale :

> Picnics, annual celebrations, and business meetings held by Sino-American S&T advocacy groups usually have someone from the S&T office in attendance along with other personnel registered to the embassy or consulate (Hannas *et al.*, 2013, *ibid.*)

[20] Au-delà d'une centaine de groupes d'intérêt, composés en majorité d'individus d'origine chinoise (citoyens américains, détenteurs de carte de résidence permanente ou de visa de travail temporaire H-1B, étudiants diplômés), ont un intérêt commun avec la Chine (Hannas, 2013 : 114). Ces groupes sont largement concentrés en Californie (Silicon Valley), là où l'acquisition de technologies depuis l'étranger est la plus intense au pays (Hannas, 2013 : 122). Le plus prestigieux et influent de ces groupes d'intérêt chinois est la Silicon Valley Chinese Engineers Association (SCEA), qui compte environ 6000 membres (Hannas, 2013, *ibid.*).

Les États-Unis envoient aussi certaines délégations de personnel d'entreprises américaines dans des secteurs stratégiques en Chine, comme ceux des produits pharmaceutiques et des logiciels (Hannas *et al.*, 2013 : 107). Que ce soit sous les auspices formels ou informels de l'État chinois, les délégations sont envoyées afin de commercialiser leur technologie en Chine (Hannas *et al.*, 2013, *ibid.*). Les officiers chinois qui occupent des postes au sein des missions diplomatiques aux États-Unis en matière de S&T agissent en rotation afin de pouvoir acquérir de l'expérience dans d'autres secteurs liés au transfert de technologies, à l'étranger ou en Chine (Hannas *et al.*, 2013, *ibid.*). Par exemple, l'un des directeurs de la China Association for International Science and Technology Cooperation a auparavant effectué un mandat de trois ans en tant que conseiller en S&T et ministre en S&T à l'Ambassade de Washington D.C., ainsi que des visites répétées dans les ambassades chinoises en Europe (Hannas *et al.*, 2013, *ibid.*).

Le réseau universitaire

Il faut remonter jusqu'au 19^{e} siècle pour s'apercevoir à quel point le réseau universitaire chinois est un outil de prédilection pour le développement technologique en Chine. Selon l'idéologie et les priorités en matière de politique étrangère qui ont ponctué les présidences chinoises à travers le temps, la Chine envoie, depuis les années 1870, des élèves de tous âges étudier principalement l'ingénierie et les sciences à l'étranger (Hannas *et al.*, 2013 : 136). À travers les époques, la Chine s'est adaptée aux différentes dynamiques mondiales, de sorte que sa stratégie s'est vue modifiée au fil du temps, en focalisant entre autres sur des pays comme le Japon, l'Union soviétique, les pays d'Europe de l'Est, l'Angleterre et les États-Unis (Hannas *et al.*, 2013 : 136-137). Globalement, de 1872 à 1978, la Chine a envoyé environ 130 000 jeunes chinois faire des études universitaires à l'étranger (Hannas *et al.*, 2013 : 137).

Toutefois, nous préviennent Hannas, Mulvenon et Puglisi, les 130 000 étudiants qui ont été recensés depuis les premiers programmes d'études à l'étranger sous la dynastie Qing (1872) jusqu'à la fin de l'ère de Mao Zedong (1976) demeurent un chiffre particulièrement faible en comparaison du nombre d'étudiants chinois qui sont allés étudier à l'étranger depuis les réformes des années 1970. La raison : les programmes d'études à l'étranger ont pris une ampleur considérable, d'autant plus que les domaines d'études stratégiques prisés par la Chine se sont élargis, ne se rattachant plus uniquement aux sciences et à l'ingénierie[21]. Selon les chiffres, entre 1978 et 2011, plus de 2,24 millions d'universitaires chinois ont fait des études supérieures aux États-Unis, parmi lesquels 818 400 (le quart) sont retournés en Chine après avoir complété leurs études (Hannas *et al.*, 2013 : 138).

Concernant les programmes d'études à l'étranger, la majorité des universités américaines ont des associations d'étudiants chinois : *la Chinese Students and Scholars Association* (CSSA) s'étend partout aux États-Unis (Hanna *et al.*, 2013 : 141). Parmi ces universités se trouvent les meilleures au pays, comme le MIT, Harvard, Stanford, Cornell, Duke, UCLA et Penn (Hanna *et al.*, 2013, *ibid.*). Ces organisations ont pour principal objectif d'intégrer les nouveaux étudiants chinois dans le pays, en organisant des activités de tout genre. Cependant, du point de vue du contre-espionnage, Hannas, Mulvenon et Puglisi mentionnent que la plus grande préoccupation au sein des services de renseignement américains est le lien qui unit ces associations étudiantes au gouvernement chinois (Hannas *et al.*, 2013 : 143). En effet, plusieurs spécialistes de la question s'interrogent sur le rapport entre les étudiants et le PCC, à savoir si les différentes filiales (196 au total en 2011) de la CSSA servent à surveiller les activités des étudiants chinois à l'étranger, en donnant des tâches particulières et en permettant

[21] Les domaines les plus populaires des étudiants chinois aux États-Unis entre 1978 et 1984 étaient la physique (31 %), l'ingénierie (23 %), les biosciences (8 %), les mathématiques (7 %) et l'informatique (4 %) (Hannas *et al.*, 2013 : 140). Pour l'année 2018-2019, les statistiques démontrent clairement les nouveaux intérêts de la Chine, alors que les mathématiques/informatique comptent pour 20 %, les affaires et la gestion (19 %), l'ingénierie (18 %), les sciences sociales (9 %) et la physique/biosciences (8 %) (Statistica, 2020)

un accès plus direct au personnel du gouvernement dans les universités. (Hannas *et al.*, 2013 : 144). Car, comme le notent les auteurs :

> The official Chinese government liaison organization for these associations are the education sections of the Chinese embassy in Washington, DC, and the consulates in New York, San Francisco, Los Angeles, Houston, and Chicago. The Chinese Embassy Education Section webpage succinctly describes the full range of their mission, including the need to "provide services and guidance for Chinese students and scholars in the USA. The Houston consulate education section website even includes links to the China Students and Scholars Associations in the states that fall under its purview (Hannas *et al.*, 2013, *ibid.*)

Non seulement la CSSA est instrumentalisée par les services diplomatiques, mais également par les services de renseignement chinois, lesquels ciblent des étudiants qui font leurs études dans des domaines stratégiques (Hannas *et al.*, 2013 : 157). Dans plusieurs cas, le MSE approche des étudiants avant même qu'ils partent pour étudier aux États-Unis, « to establish a clandestine relationship » (Hannas *et al.*, 2013, *ibid.*). Tant les étudiants que les scientifiques, qui ont déjà visité ou étudié aux États-Unis, font parfois l'objet d'un *debriefing* lorsqu'ils sont de retour en Chine (Hannas *et al.*, 2013, *ibid.*). De la même manière, le MSE recrute de façon continue et mandate certains individus dans le cadre d'échanges étudiants ou de partenariats scientifiques (comme le *Programme des 1000 talents*) dans le but d'acquérir de l'information stratégique qui puisse nourrir les ambitions nationales chinoises (Hannas *et al.*, 2013, *ibid.*).

2.2.2 La modernisation de l'appareil militaire chinois

Que ce soit par l'entremise de la création de la Commission for Science, Technology and Industry for National Defense (COSTIND) en 1982, par l'adoption du Programme 863 en 1986, par la codification formelle de la politique des « 16 caractères » en 1997, par le projet de 2015 communément nommé « MIC25 », par l'utilisation simultanée des différents services de renseignement (MSE, APL ou le Military Intelligence

Department [MID]) ou finalement, par l'établissement de sociétés-écrans aux États-Unis, l'un des dénominateurs communs de toutes ces initiatives politiques et activités opérationnelles est la volonté d'un renouvellement de la sphère militaro-industrielle (Hannas *et al,*, 2013; Roper, 2014; Qiao et Wang, 1999; Meia Nouwens et Helena Legarda, 2018)[22].

Dans la nouvelle conjoncture politique et économique qui oppose la Chine au États-Unis en matière commerciale et de droits humains au niveau régional, la confrontation militaire n'est pas nécessairement un dénouement exclu par la Chine. En effet, les contentieux liés à l'indépendance de Taiwan, ainsi qu'à la présence des États-Unis en Asie, par exemple, « prompted the Chinese to invest relentlessly in their military prowess » (Poreba, 2012 : 263). À juste titre, le rapport annuel de 2019 du Département de la Défense des États-Unis (DOD) intitulé *Military and Security Developments involving the People's Republic of China*, mentionne :

> […] China's leaders are committed to developing military power commensurate with that of a great power. Chinese military strategy documents highlight the requirement for a People's Liberation Army (PLA) able to fight and win wars, deter potential adversaries, and secure Chinese national interests overseas, including a growing emphasis on the importance of the maritime and information domains, offensive air operations, long-distance mobility operations, and space and cyber operations (DOD, 2019 : ii)

D'ici 2035, la Chine a pour objectif d'achever sa modernisation militaire, et de faire de l'APL, d'ici 2049, un appareil militaire de « classe mondiale » (DOD, 2019 : 31). Non

[22] En juillet 2020, Jun Wei Yeo, aussi connu sous le nom de « Dickson », a plaidé coupable à des accusations d'espionnage pour le compte de la Chine. L'homme, originaire de Singapour, a utilisé son cabinet de consultation politique comme société-écran pour collecter des renseignements non publics aux États-Unis. Dans son plaidoyer, Jun Wei Yeo a affirmé avoir été mandaté par les services de renseignement chinois afin de cibler certains Américains ayant une importante cote de sécurité par l'entremise du réseau social LinkedIn, pour ensuite leur demander de rédiger des rapports pour de faux clients. Recruté par les services chinois en 2015, alors qu'il était étudiant au doctorat à Singapour, Jun Wei Yeo a, selon des documents du Département de la Justice des États-Unis, dû obtenir divers renseignements sur le Département du Commerce des États-Unis, sur les nouvelles percées en matière d'intelligence artificielle, ainsi que sur les développements politiques concernant la guerre commerciale sino-américaine.

seulement des changements structuraux au plan du commandement sont prévus, mais également de nouvelles capacités militaires, comprenant des améliorations dans les stratégies de type « Déni d'accès et interdiction de zone » (A2/AD)[23], notamment en mer de Chine, et des opérations de dissuasion nucléaire et de projection de la puissance (DOD, 2019, *ibid.*). L'amélioration de la logistique des opérations conjointes et des systèmes de surveillance et de reconnaissance en temps réel, sont également des objectifs qui figurent dans l'entreprise de modernisation militaire chinoise (DOD, 2019, *ibid.*).

Pour mener à bien ces réformes, la Chine utilise une variété de stratégies faisant écho à certains principes de base de l'intelligence économique, lui permettant d'acquérir des technologies militaires étrangères (Russie, Israël et surtout les États-Unis). Voici quelques exemples tirés de l'ouvrage de Carl Roper (Roper, 2014 : 50) :

- Utiliser des membres de la famille ou des amis proches qui travaillent pour le PCC ou l'APL, et qui possèdent un rang social élevé et une autorité notoire, afin d'acheter de la technologie militaire à l'étranger.
- Profiter d'un pays tiers pour se procurer illégalement une technologie achetée légalement.
- Exercer des pressions sur les entreprises commerciales américaines pour qu'elles transfèrent illégalement à des entreprises associées (*joint ventures*) des technologies qui exigent un permis.
- Exploiter divers produits, services et technologies à double usage pour en tirer un avantage militaire.
- Détourner illégalement de la technologie à double usage à des fins militaires.
- Utiliser des sociétés-écrans établies aux États-Unis et dans d'autres pays.
- Utiliser des entreprises et des organisations commerciales comme couverture.
- Acquérir des parts dans les entreprises américaines ou tenter de devenir actionnaire majoritaire.

[23] En anglais : *Anti-Access/Area Denial*, cette stratégie, théorisée initialement par le Center for Strategic and Budgetary Assessments (CSBA) en 2003, implique le fait de contraindre un adversaire à pénétrer et à manœuvrer à sa guise dans une zone. La stratégie A2/AD comprend l'utilisation de mines terrestres, de missiles balistiques, d'armes nucléaires, chimiques, radiologiques, de missiles antinavires, antiaériens, d'attaque de type « DDoS » (attaque par déni de service), etc.

- Mener clandestinement des opérations d’espionnage dans des ministères, commissions, instituts et industries militaires conduites par des « non-professionnels » du renseignement chinois.

CHAPITRE III

LES CAS AMÉRICAIN ET CANADIEN

Ne laisse pas dormir ton attention, puisque
l'attention de ton rival est si éveillée.

Baltasar Gracian

Vers la fin des années 1990 aux États-Unis, le FBI estimait que les coûts liés à l'espionnage économique s'élevaient à 25 milliards de dollars. (Katsuya, 2019) En 2003, Steven Fink soulevait dans son ouvrage *Sticky Fingers: Managing the Global Risk of Economic Espionage* que ce genre de pratique coûtait annuellement aux entreprises américaines entre 45 et 250 milliards de dollars (Burstein, 2009 : 936). Dix ans plus tard, en 2013, le groupe de réflexion (*think tank)* américain BlackOps Partners Corporation considérait que le chiffre pouvait s'élever à 500 milliards de dollars par an (BlackOps Partners, s.d.). Durant cette même période, le Center for Responsible Trade and Enterprise (CREATe) et la société PriceWaterhouseCoopers évaluaient le coût lié au vol de secrets commerciaux entre 1 et 3 % du PIB annuel des États-Unis (Harrell, 2018). En 2017, la US China IP Commission estimait que le coût total du vol de propriété intellectuelle, y compris le cyberespionnage et la contrefaçon, valait à l'économie américaine des pertes allant de 225 à 600 milliards de dollars annuellement (Harrell, 2018). Cette hausse est attribuable, d'après le rapport NCSC de 2018, à l'expansion des réseaux informatiques basés sur l'infonuagique (*cloud computing*) et à la multiplication d'objets connectés à Internet (NCSC, 2018 : 4). Le directeur actuel du FBI, Christopher Wray, soulignait récemment : « the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China » (FBI, 2020). Il

ajoutait, à l'occasion d'une allocution à la Hudson Institute : « it's the people of the United States who are the victims of what amounts to Chinese theft on a scale so massive that it represents one of the largest transfers of wealth in human history » (FBI, 2020).

Au Canada, la tendance est similaire, mais bien moins discutée. Malgré quelques documents qui mettent en évidence la menace des activités clandestines chinoises et les secteurs les plus affectés de l'économie canadienne, l'espionnage économique en provenance de la Chine est peu documenté et très peu chiffré. L'un des seuls rapports détaillés provient d'une enquête du SCRS datant de 1995 (projet *Sidewinder*). À l'époque, il avait été estimé que de 10 à 12 milliards de dollars se perdaient chaque année au Canada, comparativement aux États-Unis où ces pertes s'élevaient à 25 milliards de dollars. (Katsuya, 2019) De manière relative, si les États-Unis sont 10 fois plus peuplés que le Canada; la relation *per capita* suggérait alors que le Canada perdait cinq fois plus que son voisin du Sud et donc, était cinq fois plus touché (Katsuya, 2019). Par rapport aux estimations des Américains sur l'impact de l'espionnage économique sur les États-Unis, le Canada perdrait aujourd'hui entre 100 et 120 milliards de dollars par année (Katsuya, 2019). Cependant, ce sont des données à interpréter avec prudence, car elles comprendraient des pertes financières d'entreprises inconnues des services de renseignement.

Aujourd'hui, le contre-espionnage n'est plus nécessairement le « parent pauvre » comme il l'a été autrefois au tournant des attentats qui ont secoué les États-Unis en 2001. En effet, lorsque le terrorisme islamique figurait au sommet des priorités des services de renseignement, les effectifs du contre-espionnage ont diminué de façon draconienne, de sorte que la majorité des ressources ont été dédiées au contre-terrorisme (Foryst, 2010 : 399-400, 410; Katsuya et de Pierrebourg, 2010 : 19)[24]. Alors que le regard était essentiellement tourné vers l'effervescence des cellules terroristes

[24] Au début des années 2000, le pourcentage de l'effectif du SCRS dédié au contre-espionnage avoisinait les 45 % (Katsuya et de Pierrebourg, 2010 : 40).

djihadistes dans les régions du Moyen-Orient, et que les craintes liées à la dissémination mondiale de ces groupes accaparaient l'esprit des dirigeants de la sécurité nationale, les activités d'espionnage économique, particulièrement depuis la Chine, n'ont néanmoins pas diminué, elles ont même augmenté.

Près de 20 ans plus tard, les tensions commerciales sino-américaines, la recherche d'un vaccin contre la COVID-19, l'arrestation et les procédures d'extradition de Meng Wanzhou, ainsi que la détention en Chine des deux ressortissants canadiens, Michael Kovrig et Michael Spavor, font de la géoéconomie l'un des champs d'étude par excellence pour expliquer les nouvelles dynamiques mondiales. La Chine se retrouve donc au cœur des préoccupations des États-Unis et du Canada. L'espionnage économique chinois devient un phénomène notoire, et met sous les projecteurs la gravité d'une problématique qui sclérose sans répit l'économie nationale américaine et canadienne depuis un bon nombre de décennies. Dans un environnement international qui pousse de plus en plus les États à entrevoir les relations économiques comme un jeu à somme nulle, les services de renseignement américains et canadiens ont pour impératif de sensibiliser la société aux risques liés à l'espionnage économique. Ces services réitèrent l'importance de protéger la propriété intellectuelle, de sécuriser les chaînes d'approvisionnement et de se méfier de certains investissements étrangers qui donnent accès à des technologies, ainsi qu'aux systèmes des infrastructures critiques.

En dépit des nouvelles tendances en matière de contre-espionnage aux États-Unis et au Canada, il est relativement nouveau de faire de l'espionnage économique chinois une priorité en matière de sécurité nationale, voire simplement de l'espionnage économique. Durant les années 1990 et 2000, ces questions faisaient l'objet d'un certain laxisme, ce qui réduisait l'importance d'implanter une véritable culture de sécurité économique au sein des secteurs public et privé (Katsuya et de Pierrebourg, 2010). L'intelligence économique comme pratique et comme état d'esprit n'a su produire un réflexe naturel chez les dirigeants, si bien qu'elle a tardé à s'imbriquer totalement dans le domaine entrepreneurial et celui du renseignement, particulièrement

dans les mécanismes de contre-espionnage. Ce faisant, le contre-espionnage américain et canadien n'a pu user d'une stratégie ralliant plus efficacement la fonction publique et le secteur privé. Une stratégie qui aurait, entre autres, permis de mieux déceler et surveiller les tendances de la politique étrangère de la Chine, ainsi que les activités des services de renseignement chinois qui posaient déjà une menace à la sécurité nationale depuis plusieurs années (Slate, 2009 : 15).

3.1 L'espionnage économique chinois aux États-Unis

Aux États-Unis, le rapport du Select Committee on U.S. National Security and Military/Commercial Concerns with The People's Republic of China, soumis par Christopher Cox en 1999 au Congrès est l'un des documents les plus importants en matière d'espionnage économique chinois. Pour la première fois, il soulignait les inquiétudes des dirigeants américains sur la question de l'espionnage chinois. Communément surnommé le « Rapport Cox », ce document gouvernemental classifié et rédigé par un comité spécial, avait pour principal objectif d'enquêter sur le transfert de technologies américaines en Chine entre les années 1980 et 1990. Le comité spécial devait établir si de l'information ou des technologies avaient véritablement été transférées à la RPC concernant l'amélioration des missiles balistiques intercontinentaux nucléaires ou la fabrication d'armes de destruction massive. Approuvé à l'unanimité par les neuf représentants de la Chambre, les conclusions de la version caviardée du rapport ont été frappantes. Dès le début du rapport il est constaté que :

> 1. la République populaire de Chine (RPC) a volé des renseignements de conception sur les armes thermonucléaires les plus avancées des États-Unis (*Cox Report*, 1999 : ii);
>
> 2. le Comité spécial juge que la prochaine génération d'armes thermonucléaires de la RPC, actuellement en cours de développement,

> exploitera des éléments d'information de conception volés aux États-Unis (*Cox Report*, 1999, *ibid.*);
>
> 3. la pénétration de nos laboratoires nationaux d'armement en RPC est une réalité depuis les dernières décennies, et se poursuit presque certainement aujourd'hui (*Cox Report*, 1999, *ibid.*)[25].

Le Rapport Cox concluait que : « despite repeated PRC thefts of the most sophisticated U.S. nuclear weapons technology, security at our national nuclear weapons laboratories does not meet even minimal standards » (*Cox Report*, 1999 : x). Dans l'ensemble, ce rapport de 200 pages a été d'une grande utilité et a permis de rendre compte d'une problématique que les comités du Congrès ne comprenaient pas bien. En 1995, les États-Unis avaient découvert que la RPC avait volé de l'information sur la conception des ogives W-88 Trident D-5 et d'autres types d'ogives thermonucléaires. Non seulement le Congrès a-t-il tardé à se pencher sur ces cas d'espionnage, mais l'administration Clinton a avoué au comité dirigé par Christopher Cox n'avoir été renseignée sur ces échecs du contre-espionnage qu'en 1998 (*Cox Report*, 1999 : xi).

Qui plus est, le comité spécial exposait que « […] given the great significance of the PRC thefts, the Select Committee is concerned that the appropriate committees of the Congress were not adequately briefed on the extent of the PRC's espionage efforts » (*Cox Report*, 1999, *ibid.*). De fait, deux constats ont été faits à ce sujet : 1) la communauté du renseignement américain manque de ressources pour faire face aux activités clandestines de la Chine; et 2) les ressources du FBI dédiées à la surveillance de la RPC ne sont pas proportionnelles au nombre de visiteurs, d'étudiants, de diplomates et de représentants d'entreprises chinoises sur le territoire américain (*Cox Report*, 1999 : xxxiv).

Si les conclusions du Rapport Cox précipitaient entre autres la mise en place de mécanismes de contre-espionnage pour traiter l'espionnage économique chinois aux

[25] Traduction libre

États-Unis, 15 ans plus tard, le rapport de l'IP Commission de 2013 rendait également une analyse peu encourageante concernant ces crimes économiques. En effet, le document dédié au vol de la propriété intellectuelle faisait les constats suivants : 1) les pertes annuelles sont comparables aux coûts annuels d'exportation vers l'Asie (environ 300 milliards de dollars US); 2) des millions d'emplois ne peuvent être créés aux États-Unis; 3) le PIB annuel américain ralentit; et 4) la menace du vol de la propriété intellectuelle diminue l'incitation à innover (*IP Commission Report*, 2013 : 1).

En outre, le rapport de 2013 soulignait le rôle de la Chine, qui était alors jugée responsable de 50 à 80 % du vol de propriété intellectuelle aux États-Unis (*IP Commission Report*, 2013 : 3). Selon le document, les preuves que la Chine était le principal pays à s'adonner à ce genre de pratique en sol américain provenaient de diverses sources, y compris le pourcentage des cas judiciaires impliquant la Chine, les rapports du représentant américain au commerce, les études d'entreprises spécialisées et de groupes industriels, ainsi que les études parrainées par le gouvernement des États-Unis (*IP Commission Report*, 2013, *ibid.*). Il y était également mentionné que les objectifs nationaux de la Chine encourageaient le vol de propriété intellectuelle et qu'il existait de grandes faiblesses dans les divers systèmes juridiques et de brevets, diminuant à cet effet, la protection de la propriété intellectuelle (*IP Commission Report*, 2013, *ibid.*).

Ce rapport, rédigé par des membres des secteurs public et privé, de la sécurité nationale, des affaires étrangères, des milieux universitaire et politique, concluait que les « remèdes » existants ne peuvent véritablement circonscrire l'espionnage économique chinois. Les conclusions étaient les suivantes (*IP Commission Report*, 2013, *ibid.*) :

- *Le court cycle de vie des produits* – Même dans les meilleurs appareils judiciaires, la lenteur des recours juridiques en cas d'infraction à la propriété intellectuelle ne répond pas aux besoins des entreprises dont les produits ont une courte durée de vie et des cycles de profit rapides.

- *La capacité institutionnelle* – La capacité institutionnelle de traiter les affaires concernant l'atteinte aux droits de la propriété intellectuelle est inadéquate, particulièrement à l'égard des pays en développement. L'un des exemples est la pénurie de juges formés sur le sujet.

- *L'approche américaine envers la Chine en matière de propriété intellectuelle* – Les améliorations apportées au fil des ans n'ont pas protégé de manière significative la propriété intellectuelle américaine, et il n'y a pas non plus de preuve que des améliorations substantielles sont imminentes. En fait, les cyberattaques se multiplient.

- *Les limites des accords commerciaux* – Bien que les États-Unis se soumettent aux règlements de l'Organisation mondiale du commerce (OMC), plusieurs conflits commerciaux n'ont pas débouché sur des résolutions efficaces. Les accords bilatéraux et régionaux de libre-échange ne sont pas non plus une panacée.

- *Les actions entreprises par le Congrès* – Des mesures ont été prises récemment, à la fois pour traiter le problème comme une priorité politique et pour resserrer la loi américaine sur l'espionnage économique. Ce sont des étapes positives. Un projet de loi au Congrès, qui permettrait un plus grand partage de l'information entre le gouvernement et les entreprises privées, doit être adopté et modifié si nécessaire. Tous ces efforts, cependant, ne changeront pas la structure d'incitation sous-jacente pour les voleurs de propriété intellectuelle, et auront donc un effet limité.

Malgré des actions plus concrètes mises de l'avant par l'administration Obama, le rapport de 2017 de l'IP Commission souligne principalement la persistance du vol de la propriété intellectuelle aux États-Unis (*IP Commission Report*, 2017 : 7). En effet, même si l'administration Obama et le Congrès ont mis en place plusieurs politiques pour réduire le vol de la propriété intellectuelle américaine, selon les recommandations du rapport de 2013 de l'IP Commission, le problème continue de scléroser les États-Unis, étant donné une faible application de la loi à l'égard des pratiques industrielles étrangères, selon les commissaires du rapport de 2017. Précisément, ces derniers mentionnent que les forces de l'ordre n'ont pas les capacités suffisantes pour protéger l'entièreté du milieu américain des affaires et que les acteurs étrangers impliqués dans

le vol de propriété intellectuelle sont rarement amenés devant les tribunaux (*IP Commission Report*, 2017 : 8).

En bout de ligne, l'espionnage économique aux États-Unis continue d'être un problème qui semble pouvoir se circonscrire en grande partie par la révision des lois fédérales et l'intensification des poursuites judiciaires (Crosston, 2015 : 119). En effet, comme nous le verrons, les mécanismes de protection américains en réponse à l'espionnage économique depuis le début des années 1990 impliquent presque uniquement le raffermissement de la loi et l'augmentation des ressources, au détriment de résolutions qui révisent directement la structure socioéconomique, ainsi que la posture stratégique américaine en matière d'intelligence économique. Voici quelques cas d'espionnage économique chinois qui se sont produits aux États-Unis depuis 2010 :

Tableau 1
Cinq cas d'espionnage économique chinois survenus aux États-Unis
entre 2010 et 2015[26]

2010	En février 2010, Dogfan « Greg » Chung, 73 ans, ancien ingénieur de Boeing, a été condamné à près de 16 ans de prison pour vol de secrets dans le domaine de l'aérospatial au profit de la RPC. Chung, originaire de Chine et naturalisé américain, détenait une habilitation de sécurité « secrète » lorsqu'il travaillait chez Rockwell et Boeing dans le cadre du programme de la navette spatiale. Il a pris sa retraite de l'entreprise en 2002, mais l'année suivante, il est retourné chez Boeing en tant qu'entrepreneur, un poste qu'il a occupé jusqu'en septembre 2006. Au cours du procès, le gouvernement a prouvé que Chung avait volé des secrets commerciaux, ainsi que divers matériaux relatifs à la navette spatiale et à la fusée Delta IV appartenant à Boeing. Il s'agissait du premier procès d'espionnage économique de l'histoire des États-Unis. (FBI, 2010).

[26] Les exemples du tableau 1 proviennent du site Web du FBI et de celui du Département de la Justice. Les exemples cités ont tous été traduits librement.

2013	En mars 2013, Sixing Liu, alias « Steve Liu », 49 ans, un entrepreneur de la Défense basé au New Jersey, a été condamné pour vol de secrets commerciaux et exportation de technologies militaires américaines sensibles à la RPC. En 2010, Liu a volé des milliers de fichiers électroniques à son employeur, L-3 Communications, situé à Budd Lake, au New Jersey. Les fichiers volés détaillaient les performances et la conception des systèmes de guidage des missiles, des roquettes, des localisateurs de cibles et des véhicules aériens sans pilote. Liu a volé les dossiers pour obtenir un futur emploi au sein de la RPC. Dans le cadre de ce plan, Liu a présenté des exposés sur la technologie dans plusieurs universités de la RPC, et a participé à des conférences organisées par le PCC (FBI, 2013).
2014	Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu et Gu Chunhui, officiers de l'unité 61398 du troisième département de l'APL, ont été accusés d'avoir mené des opérations d'espionnage économique contre des sociétés américaines à des fins commerciales entre 2006 et 2014. L'acte d'accusation allègue que Wang, Sun et Wen ont piraté ou tenté de pirater des entités américaines, tandis que Huang et Gu ont appuyé leurs opérations. Les pirates informatiques ont volé des secrets commerciaux qui auraient été particulièrement bénéfiques pour les entreprises chinoises. Ils ont également intercepté des communications internes sensibles (DOJ, 2014).
2014	En juillet 2014, Walter Lian-Heen Liew, alias Liu Yuanxuan, un Californien de 56 ans, a été condamné à 15 ans de prison pour de multiples accusations liées au vol de secrets commerciaux de la compagnie DuPont au profit de sociétés d'État chinoises. Les secrets commerciaux concernaient une technologie de production de dioxyde de titane (TiO_2). Les éléments de preuve présentés au procès ont montré qu'au début des années 1990, Liew a rencontré le PCC et a été informé que le développement de la technologie impliquant du TiO_2 était une priorité pour le pays. Le procédé du TiO_2 de DuPont produit du tétrachlorure de titane, un matériau à usage militaire et aérospatial. Liew savait que DuPont avait développé la *technologie* TiO_2 au cours de nombreuses années de R&D et a formé une équipe d'anciens employés de DuPont pour transmettre cette technologie à des entités de la RPC. Liew et d'autres partenaires ont exécuté des contrats avec des entités publiques de la RPC. Précisément, ils ont obtenu et vendu les secrets commerciaux de DuPont aux sociétés du groupe Pangang pour plus de 20 millions de dollars (DOJ, 2014).
2015	En mai 2015, Wei Pang and Hao Zhang, deux professeurs chinois, ont été accusés d'espionnage économique et de vol de secrets commerciaux

	au profit d'universités et d'entreprises contrôlées par la RPC. Selon l'acte d'accusation, Pang et Zhang, ressortissants de la RPC, se sont rencontrés dans une université américaine du sud de la Californie au cours de leurs études doctorales en génie électrique. Pang et Zhang ont mené des recherches et ont participé au développement de résonateurs acoustiques à couches minces (FBAR), le tout, financé par la Defense Advanced Research Projects Agency (DARPA) des États-Unis. Après avoir obtenu leur doctorat vers 2005, Pang a décroché un emploi en tant qu'ingénieur chez Avago Technologies (Avago) au Colorado et Zhang a obtenu un emploi en tant qu'ingénieur chez Skyworks Solutions Inc. (Skyworks) dans le Massachusetts. En 2006 et 2007, Pang et Zhang ont élaboré un plan d'affaires, et ont commencé à solliciter des universités en RPC. Ces derniers cherchaient des possibilités d'emploi pour exporter la technologie FBAR en Chine. Selon l'acte d'accusation, Pang et Zhang, ainsi que d'autres partenaires, ont établi des relations avec des fonctionnaires de l'Université de Tianjin. L'Université de Tianjin est l'une des principales universités du ministère de l'Éducation de la RPC (DOJ, 2015).

3.2 L'espionnage économique chinois au Canada

Pendant de nombreuses années, du côté canadien, lorsqu'il était question d'espionnage économique, l'adage par excellence des services de renseignement au Canada (GRC et SCRS) et de certains chefs d'entreprise se résumait à : « *see no evil, speak no evil* » (Katsuya et de Pierrebourg, 2010 : 20-22). Jumelé à cette devise qui balaye du revers de la main les crimes de « cols blancs », les ressources du contre-espionnage au SCRS ont substantiellement maigri, et ce, au moment où le terrorisme devenait la priorité numéro un des services de renseignement et des corps policiers canadiens (Katsuya et de Pierrebourg, 2010 : 19, 345). Il faut alors remonter à la fin des années 1990 pour trouver l'un des seuls rapports rendus public par les autorités canadiennes. Ce rapport, toutefois très controversé, n'a jamais eu la portée médiatique espérée.

En mai 1996, la Direction générale de l'analyse criminelle de la GRC et la Direction générale de l'analyse et de la production du SCRS amorçaient conjointement un projet dont l'objectif était d'évaluer l'ampleur de la menace que représentaient l'acquisition et le contrôle des entreprises canadiennes par des membres de triades affiliées aux services de renseignement chinois (Sidewinder Report, 1997 : iii). Communément appelé le projet « Sidewinder », ce rapport révélait l'existence d'opérations d'influence visant des politiciens canadiens, de vol de hautes technologies, de blanchiment d'argent, ainsi que de prise de contrôle de compagnies immobilières, médiatiques, etc. (Sidewinder Report, 1997 : 6-10).

Les conclusions du rapport étaient si controversées que certains gestionnaires du SCRS les ont « édulcorées et réécrites avant qu'une version aseptisée du rapport, (rebaptisée « Echo »), ne soit distribuée à d'autres organismes gouvernementaux en 1999 » (Mitrovica et Sallot, 2000)[27]. La première version du rapport faisait la recommandation d'un élargissement du groupe de travail (GRC-SCRS) pour y inclure le ministère des Affaires étrangères (devenu Affaires mondiales Canada [AMC]), Immigration, Réfugiés et Citoyenneté Canada (IRCC) et l'Agence des services frontaliers du Canada (ASFC). Cependant, cette recommandation ne s'est jamais réalisée. Écartée dès le départ, la première version du projet Sidewinder a été étiquetée comme une théorie du complot, dont les conclusions « potentiellement explosives » étaient fondées sur un manque de preuves flagrant (Mitrovica et Sallot, 2000). Dans la foulée, plusieurs se sont posé la question à savoir s'il y avait eu ingérence ou une quelconque pression politique extérieure. Car, de l'autre côté de la frontière, aux États-Unis, le Rapport Cox n'a jamais rencontré une pareille contestation des services de renseignement, ni des instances politiques.

Dans son rapport annuel de 1999-2000, le Comité de surveillance des activités de renseignement de sécurité (CSARS) mentionnait :

[27] Traduction libre

> Le Comité n'a trouvé aucune preuve de la prétendue ingérence politique. Aucun des documents et dossiers examinés, aucune des entrevues menées ni des observations recueillies ne permettent de croire en une telle ingérence, réelle ou présumée. Le projet Sidewinder n'a pas été abandonné : il a été retardé après qu'on eut jugé le rapport insatisfaisant (Rapport du CSARS, 1999-2000)
>
> Quant à la première ébauche du rapport Sidewinder, nous l'avons trouvée très boiteuse à presque tous les égards. Elle dérogeait aux normes de rigueur professionnelle et analytique les plus élémentaires. Les mesures prises par le Service pour rehausser la qualité de ses futurs travaux de collaboration avec la GRC au projet Sidewinder étaient appropriées (Rapport du CSARS, 1999-2000)

L'affaire Sidewinder a continué de faire couler beaucoup d'encre pendant quelque temps, et encore aujourd'hui, il est difficile de connaître les véritables raisons qui ont abouti à l'avortement de la première version du rapport (Katsuya et de Pierrebourg, 2010 : 206). Toutefois, il faut garder à l'esprit que durant la même période, le premier ministre du Canada de l'époque, Jean Chrétien, privilégiait le commerce avec la Chine, et en avait même fait l'une de ses priorités (Katsuya et de Pierrebourg, 2010 : 207). Également en 1997, André Desmarais, qui était nouvellement président et co-chef de la direction de Power Corporation, est devenu membre du conseil d'administration de la société d'État China International Trust Investment Company (CITIC). Ce conglomérat chinois, fondé avec l'aval de Deng Xiaoping en 1979, avait pour principaux buts d'attirer et d'utiliser :

> « […] foreign capital, introducing advanced technologies, and adopting advanced and scientific international practice in operation and management thus building up good reputation and image both home and abroad with a remarkable performance » (CITIC Limited, s.d.)[28]

[28] La CITIC possède 44 filiales, dont la China CITIC Bank, la CITIC Limited, la CITIC Trust et la CITIC Merchant en Chine, à Hong Kong, aux États-Unis, au Canada, en Australie et en Nouvelle-Zélande.

À ce titre, Agnès Andrésy, rédactrice en chef d'*Arcanes de Chine*, écrivait dans son ouvrage *Princes rouges – Les nouveaux puissants de la Chine* (2004), que la direction de la CITIC, dont les affaires touchent notamment les secteurs du transport, des télécommunications et de l'armement, est reconnue pour abriter un grand nombre d'agents de renseignement chinois du 2PLA (Andrésy, 2004, cité par Katsuya et de Pierrebourg, 2010, *ibid.*). Cette tactique était intégrée à la compagnie chinoise, à la demande de Deng Xiaoping, alors qu'il était à l'époque chef de l'état-major de l'APL (Andrésy, 2004, cité par Faligot, 2019 : 204).

Hormis la controverse entourant la publication du rapport Sidewinder, rares ont été les documents, les directives détaillées ou même les audiences qui se sont penchées publiquement sur l'enjeu entourant l'espionnage économique chinois au Canada durant les années 2000 et début 2010. Quelques publications du SCRS ont traité du sujet, notamment dans les séries *Commentaire* et *Regards sur le monde*. Néanmoins, l'information « grand public » est longtemps demeurée évasive. Ce silence a certes été rompu à quelques reprises par les commentaires accusateurs de Peter McKay, ancien ministre des Affaires étrangères, et de l'ancien premier ministre du Canada, Stephen Harper, envers la Chine en 2006, ainsi que par ceux de Jim Judd, alors directeur du SCRS, devant le comité sénatorial permanent de la sécurité nationale en 2007 (Katsuya et de Pierrebourg, 2010 : 200-201). Cependant rien de véritablement substantiel ne s'est matérialisé dans les années qui ont suivi.

Depuis la fin des années 2010, les services concernés sur la question de l'espionnage économique au Canada affichent un intérêt grandissant pour cette question. Du moins, ces derniers semblent communiquer plus aisément avec le public sur ce genre d'enjeu. Entre autres, par souci de transparence, le SCRS comme le CST fournissent désormais des rapports publics davantage détaillés, comme en témoignent d'ailleurs les nombreux documents de sensibilisation relatifs à l'espionnage économique publiés sur leurs sites Web respectifs et sur les médias sociaux. À titre d'exemple, une récente vidéoconférence, organisée par le SCRS et la Chambre du Commerce du Canada, a été

présentée publiquement afin de sensibiliser les Canadiens concernant les menaces étrangères qui ont un impact sur la sécurité économique du Canada. L'espionnage économique semble désormais attirer de plus en plus l'attention des dirigeants de la sécurité nationale. À ce titre, le récent rapport du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), présenté au premier ministre en 2019, met de l'avant la menace que représente la Chine en termes d'ingérence étrangère (CPSNR, 2019). Largement caviardé, le rapport présente toutefois des conclusions sans équivoque, parmi lesquelles :

> […] les entités chinoises, incluant les entreprises de l'État et du secteur privé, de même que les citoyens chinois (peu importe s'ils sont résidents d'autres pays) [coopèrent] avec les Services du renseignement de la RPC et le gouvernement en général sur les questions de sécurité nationale [...] La *Loi sur le renseignement national* s'applique aussi aux entités chinoises et aux particuliers chinois qui œuvrent à l'extérieur de la Chine [...] La loi sur le renseignement chinois crée un cadre juridique évident de coopération entre les services du renseignement de la RPC, les entreprises et les particuliers chinois (CPSNR, 2019 : 68)

ou encore :

> […] les CSSA représentent un important mécanisme de soutien pour les étudiants étrangers et fournissent un réseau social et professionnel aux étudiants. […] Toutefois, la population est de plus en plus concernée au sujet de la relation entre les associations [universitaires] et les ambassades, ou les consulats de la RPC, puisque les CSSA représentent l'un des principaux moyens pour les autorités chinoises de guider les étudiants et les universitaires chinois en ce qui a trait aux études à court terme à l'étranger (CPSNR, 2019 : 80)

L'intérêt des services de sécurité canadiens pour la Chine est relativement nouveau, mais leur réaction arrive en retard. Si les entreprises canadiennes sont aujourd'hui de plus en plus sensibilisées aux conséquences à plus long terme de l'espionnage économique, la création des moyens de protection juridique au Canada contre ces activités ont tardé, et une fois mis en vigueur, ils n'ont que partiellement traité le

problème. Voici quelques cas d'espionnage économique survenus au Canada ces dernières années[29] :

Tableau 2
Cinq cas d'espionnage économique chinois impliquant le Canada et les États-Unis entre 2012 et 2018

2012	Entre avril 2011 et décembre 2012, Hongwei Wang, 43 ans, résident de L'Île-Perrot, travaillait dans une entreprise pharmaceutique à Candiac. Connu des services de renseignements américains, Hongwei a été arrêté en 2012 au Vermont. Le FBI a effectué une saisie, lors de laquelle ses agents ont trouvé 880 enveloppes, un cahier contenant des informations sur l'emplacement géographique de champs de maïs et plusieurs photos de champs agricoles et de laboratoires de compagnies comme Monsanto et Pioneer. Hongwei volait des semences génétiquement modifiées et brevetées en creusant à la main dans les champs. Celui-ci faisait partie d'un réseau clandestin (Shaoming Li, Yong Li, Lei Wang et Jian Ye), lequel travaillait pour un conglomérat agricole chinois. Hongwei a finalement été relâché, et a pu se soustraire aux accusations criminelles en fuyant dans son pays natal. Selon les informations du FBI, les pertes estimées représentent cinq à huit années de R&D, l'équivalent de 30 à 40 millions de dollars (Larouche, 2020).
2014	Le Conseil national de recherches du Canada (CNRC) a été visé par une cyberattaque en provenance de la Chine, selon ce qu'a rapporté le Conseil du Trésor. Tous les détails concernant cette opération de cyberespionnage n'ont pas été révélés. Toutefois, on estime qu'une grande quantité d'informations sensibles pourraient avoir été dérobées. Lors de l'attaque, le CNRC travaillait sur un système de chiffrement capable de détecter et de contrer plus efficacement ce genre d'attaque. Le CNRC se penchait précisément sur le développement de la communication quantique et les technologies satellites. L'attaque a été découverte par le Centre de la sécurité des télécommunications (CST) (Bronskill, 2014; Barton, 2014).

[29] Les exemples cités proviennent de diverses sources journalistiques et concernent, pour la plupart, tant le Canada que les États-Unis.

2018	Ishiang Shih, professeur à l'université McGill et ingénieur électrique, et Yi-Chi Shih, son frère diplômé de l'université d'Ottawa, résident californien, et lui aussi ingénieur électrique, ont été accusés par la justice américaine d'avoir commis plusieurs infractions liées au transfert de puces informatiques vers la Chine. Ces derniers faisaient partie d'un réseau clandestin qui exportait vers la Chine des circuits intégrés de calibre militaire (circuits intégrés micro-ondes monolithiques [MMIC]) dans l'objectif de contribuer au développement de missiles chinois. Les procureurs américains ont allégué que les frères Shih opéraient illégalement dans le but d'obtenir ces puces informatiques pour ensuite les envoyer à une entreprise chinoise pour laquelle les deux frères avaient préalablement travaillé. Cette compagnie, Chengdu Gastone Technology Company (CGTC), a été ajoutée en 2014 à la liste de contrôle des exportations du DOC, parce qu'elle se serait procurée illégalement des technologies à des fins militaires non autorisées (Blackwell, 2019; Larouche, 2020).
2018	Zhu Hua et Zhang Shilong, pirates informatiques du groupe APT10 associé au MSE, ont mené entre 2006 et 2018 des opérations de cyberespionnage dans les systèmes informatiques de 12 entreprises canadiennes des secteurs miniers, médicaux, de la finance et des télécommunications. Zhu et Zhang travaillaient pour la firme Huaying Haital Science and Technology Development, une firme intimement liée au PCC. Plus largement, les opérations de cyberespionnage ont visé plus de 45 entreprises dans le monde, et les informations soutirées impliquaient notamment des données concernant l'aviation, les technologies spatiales et les produits pharmaceutiques (DOC, 2018).
2018	Shuren Qin, entrepreneur chinois, résident de Wellesley dans le Massachussetts, a, entre autres, été accusé d'avoir fourni illégalement à l'APL des hydrophones (dispositifs militaires utilisés pour détecter le son sous l'eau). Qin opérait par l'entremise de diverses sociétés en Chine, dont LinkOcean Technologies, une firme de distribution chinoise qui importe des biens et des technologies ayant des applications sous-marines depuis les États-Unis, l'Europe et le Canada (Ontario, Nouvelle-Écosse et Terre-Neuve-et-Labrador). Selon l'acte d'accusation, Qin a reçu des instructions claires de l'APL et de l'université Northwestern Polytechnical (NWPU), un institut de recherche militaire chinois, dont les liens avec l'APL sont très étroits. Toujours selon l'acte d'accusation, de juillet 2015 à décembre 2016, Qin a exporté vers la Chine (NWPU) plus de 60 hydrophones sans les licences d'exportation nécessaires (DOC, 2018; Larouche).

3.3 Les mécanismes de protection américains et canadiens

Dès le début des années 1990, la sécurité économique s'est rapidement imbriquée dans les intérêts nationaux, ainsi que dans la sécurité nationale des États-Unis (Roper, 2014 : 153; Bellocchi, 2001 : 366). Dans la foulée, plusieurs programmes et politiques ont été mis en place sous l'administration Clinton, afin d'appréhender l'espionnage économique, comme l'*Economic Counterintelligence Program* du FBI en 1994 : un programme de contre-espionnage qui était dédié au renseignement de menaces économiques en provenance de l'étranger (Roper, 2014 : 154).

Deux ans plus tard, en 1996, le Congrès adoptait l'*Economic Espionage Act* (EEA) dans un contexte où le Département de la Justice et plusieurs compagnies américaines estimaient que la loi relative aux secrets commerciaux des entreprises était inadéquate et ne traitait pas des nouvelles réalités économiques (Bellocchi, 2001 : 366). Ce faisant, la loi sur le secret commercial est devenue sous la juridiction des affaires criminelles fédérales pour la première fois dans l'histoire des États-Unis. Bien que les activités criminalisées par le EEA ont toujours été interdites par la loi de l'État, et ce, en conformité avec le code d'éthique du SCIP, les conséquences ont néanmoins changé. En d'autres mots, comme le souligne Richard Horowitz, « an activity that had always been a violation of state trade secret law can now result in not only state civil liability but federal criminal liability as well » (Horowitz, 1999 : 86).

S'en est suivi, en 1997, le *No Electronic Theft Act* (NET, H.R. 2265), signé par l'administration Clinton. Le NET avait pour principales utilités d'améliorer la protection entourant le droit d'auteur (*copyright*) et le droit des marques (*trademark*), ainsi que d'élargir les critères des poursuites judiciaires, afin de poursuivre en justice une plus grande variété de cas à l'égard du vol d'information économique (Roper, 2014 : 155). Le NET avait pour objectif de couvrir de nombreux éléments relatifs aux domaines scientifiques, médicaux et technologiques des États-Unis. Parmi les

nouveaux éléments protégés, se trouvaient : la fraude informatique, la contrefaçon (CD, DVD, vêtements, accessoires, puces informatiques, médicaments, produits de luxe, etc.), les lignes de cellules d'ADN, la copie illégale de films, la recherche sur les microprocesseurs, les dispositifs d'interception de télévision par satellite piratés, le piratage de logiciels, les plans de machines à ultrason, etc. (Roper, 2014 : 156).

En 2001, deux semaines avant de quitter le Bureau ovale, le président Clinton adoptait la directive présidentielle 75 (PDD 75), nommée *U.S. Counterintelligence Effectiveness – Counterintelligence for the Twenty-first Century*. Cette directive impliquait des mesures précises permettant à la communauté du renseignement américain d'être mieux outillée en matière de contre-espionnage. La PDD 75 entrevoyait un système de renseignement davantage prévoyant et efficace en termes de coordination entre agences de sécurité nationale. Ce faisant, le National Counterintelligence Executive (NCIX) a été créé pour remplacer le National Counterintelligence Executive (NACIC), dont le nouveau rôle était de servir en tant que chef du contre-espionnage au niveau national, et à titre de coordonnateur des missions du contre-espionnage américain (Roper, 2014 : 154). L'une des principales nouveautés du NCIX était son plus large intérêt pour le secteur privé, lequel a été marqué notamment par les campagnes de sensibilisation dans les organisations de sécurité du secteur privé comme l'American Society for Industrial Security et la National Classification Management Society (Roper, 2014 : 155).

Suivant l'*Intellectual Property Rights Enforcement Act* de 2005 et le *Prioritizing Resources and Organization for Intellectual Property Act* (PRO-IP Act, H.R. 4279) de 2008, l'administration Obama publiait en 2010 le *Joint Strategic Plan on Intellectual Property Enforcement*, un rapport qui contenait un plan de coordination des ressources et des priorités des États-Unis, afin de soutenir le renforcement des protections en matière de propriété intellectuelle. Ce rapport était, entre autres, le fruit d'un travail conjoint entre de nombreuses agences américaines, comme le U.S. Department of Agriculture (USDA), le Department of Commerce (DOC), le Department of Health

and Human Services (HHS), le Department of Homeland Security (DHS), le Department of Justice (DOJ), le Department of State (DOS), l'Office of the U.S. Trade Representatives (USTR) et le U.S. Copyright Office. De ce travail a émergé un plan d'action qui se décline en six axes : 1) montrer l'exemple; 2) améliorer la transparence; 3) garantir l'efficience et la coordination; 4) renforcer les droits internationaux; 5) sécuriser la chaîne d'approvisionnement; et 6) créer un gouvernement axé sur les données. (*Joint Strategic Plan on Intellectual Property Enforcement*, 2010 : 21-22)

Qui plus est, en réponse aux activités d'espionnage économique, le gouvernement américain soutient le secteur privé de diverses manières, par l'entremise de ses départements et agences depuis les années 1990. Ces « joueurs » majeurs, qui participent au contre-espionnage américain en coopérant avec certaines entreprises, sont les suivants : le Federal Bureau Investigation (FBI) (programme ANSIR[30]), le Department of State (DOS) (coentreprise OSAC[31]), la Central Intelligence Agency (CIA), la Defense Intelligence Agency (DIA), le Department of Defense (DOD), la National Reconnaissance Office (NRO), le ONCIX (maintenant sous la coordination du NCSC), le Department of Energy (DOE), le Department of Commerce (DOC), le U.S. Customs et la National Aeronautics and Space Administration (NASA) (Roper, 2014 : 164-167).

[30] Le programme « ANSIR » (*Awareness of National Security Issues and Response*) est une mission lancée par le FBI dans les années 1990 qui « attempts to reduce American vulnerability by providing awareness information on the techniques used by foreign intelligence services to collect proprietary economic information » (Waguespack, 2001).

[31] Depuis 1985, « the Overseas Security Advisory Council (OSAC), a joint venture between the Department of State and the U.S. private sector, created by then Secretary of State George P. Shultz under the Federal Advisory Committee Act to interact on overseas security problems of mutual concern. Objectives of this joint venture are: to establish a continuing liaison between security officials in both the private and public sector; to provide for regular exchanges of information concerning developments in the overseas security environment; recommend methods for planning and implementation of security programs abroad; and recommend methods to mitigate risks to American private sector interests worldwide » (OSAC, s.d.).

En dressant un bilan (non exhaustif) des nombreux mécanismes de protection américains à l'égard de l'espionnage économique, on peut déjà constater que les États-Unis ont entrepris plusieurs actions au cours des dernières décennies, en réaction à la problématique, afin de l'enrayer, ou du moins, l'amoindrir. Parmi les lois fédérales qui peuvent s'appliquer, se trouvent l'EEA, les diverses lois qui protègent le droit d'auteur et les brevets, le *Digital Millennium Copyright Act* (DMCA), une loi de 1998 qui criminalise la production et la distribution de technologies, d'appareils ou de services visant à contourner les mesures de protection du droit d'auteur, le *Trade Secret Act* (TSA), etc. (Roper, 2014 : 153). Par contre, hormis toutes les lois applicables, l'établissement de nouvelles lois demeure un processus lent. Car, bien que le Congrès s'intéresse aux questions liées à l'espionnage économique, notamment en tenant plusieurs audiences sur le sujet et en publiant des rapports, les solutions proposées provoquent souvent un effet discordant et conséquemment, celles-ci peinent à trouver un véritable consensus au sein des décideurs (Roper, 2014 : 153).

Dans un même temps, comme le soutient Aaron Burstein, l'EEA et d'autres mesures législatives du même genre sont incomplètes, puisque même si ces lois criminalisent davantage l'espionnage économique, elles n'ont jamais réellement harmonisé les incitatifs commerciaux et les préoccupations de sécurité nationale (Burstein, 2009 : 34-42, cité par Crosston, 2015 : 113). En d'autres termes, si le gouvernement américain n'accompagne pas plus efficacement les entreprises dans un contexte économique libre-échangiste, par exemple, en ne les sensibilisant pas assez aux activités clandestines étrangères, les États-Unis sont alors condamnés à une augmentation des cas d'espionnage économique à leurs dépens (Crosston, 2015, ibid.). Aaron Burstein ajoute que la principale faiblesse du cadre légal américain entourant l'espionnage économique est qu'il est trop lourdement axé sur la section punitive de l'EEA (Burstein, 2009 : 57)[32]. Conséquemment, les dispositifs juridiques ne se focalisent pas

[32] La section 1831 (18 U.S. Code § 1831) concerne la protection du secret commercial. Précisément, elle incrimine l'appropriation illicite de secrets commerciaux comprenant le complot, en vue de détourner

suffisamment sur l'essentiel de la problématique, à savoir que les détenteurs de secrets commerciaux n'ont pas les ressources et les incitations nécessaires pour protéger leurs renseignements contre les menaces sophistiquées, que les organismes d'application de la loi et de renseignement dépendent de la coopération volontaire du secteur privé et qu'il y a une absence de normes concernant la collecte d'information par l'intermédiaire des réseaux (Burstein, 2009, *ibid.*; Crosston, 2015 : 114). Nathaniel Minott renchérit en expliquant que les sanctions sévères de l'EEA ne ciblent pas correctement les acteurs clés (Minott, 2011 : 202). L'EEA n'est pas outillé efficacement pour dissuader et punir l'espionnage économique parrainé par l'État, étant donné qu'il s'agit d'une loi nationale dont l'application incombe uniquement aux institutions juridiques des États-Unis. En d'autres termes, la loi intérieure des États-Unis semble insuffisante pour traiter de manière efficace l'espionnage économique chinois.

Au Canada, le problème est essentiellement le même qu'aux États-Unis, notamment en ce qui a trait à la portée de la loi à l'égard des contrevenants étrangers. C'est ce que soutiennent d'ailleurs Emir Crowne et Tasha De Freitas lorsqu'ils mentionnent que les dispositions du Code Criminel canadien sont si limitées qu'elles ne saisissent que les activités d'individus, et non celles des entreprises ou des sociétés qui ont préalablement incité des gens à faire de l'espionnage (Crowne et De Freitas, 2013 : 194). Cela renforce les propos de Melanie Reid qui explique que les poursuites en matière d'espionnage sont difficiles à intenter, puisque l'établissement de la preuve implique de démontrer que la partie défenderesse savait que ses actions bénéficieraient à une entité étrangère (Reid, 2016 : 803).

---

des secrets commerciaux et l'acquisition ultérieure de ces secrets commerciaux détournés, avec la connaissance ou l'intention que le vol profite à une puissance étrangère. Les sanctions pour violation sont des amendes pouvant s'élever à 500 000 USD par infraction, des peines d'emprisonnement pouvant aller jusqu'à 15 ans pour les particuliers, et des amendes pouvant atteindre 10 millions USD pour les organisations.

À la grande différence de son voisin du Sud, le Canada ne s'est pas doté d'un cadre juridique singulier pour traiter l'espionnage économique dès le tournant de la guerre froide. (Katsuya et de Pierrebourg, 2010 : 21) C'est en 2001 que la *Loi antiterroriste*, intitulée Projet de loi C-36, est venue modifier le Code Criminel en y apportant certains changements comme la création de la *Loi sur la protection de l'information* (anciennement la *Loi sur les secrets officiels*)[33]. Précisément, les sections 19 et 20 de la *Loi sur la protection de l'information* venaient définir l'espionnage économique ainsi que les menaces et accusations violentes, au profit d'entités étrangères ou d'un groupe terroriste. En tout état de cause, le Code Criminel restait encore le seul et dernier retranchement pour couvrir les enjeux qui touchaient l'espionnage économique (Katsuya et de Pierrebourg, 2010 : 21). Depuis ce temps, le cadre juridique n'a pas évolué corrélativement aux changements technologiques. Ce faisant, la loi canadienne offre toujours peu de protection, tant pour les individus que pour les entreprises victimes d'espionnage économique (Crowne et De Freitas, 2013-2014 : 192, 198).

La section 19 de la *Loi sur la protection de l'information* se lit comme suit (Loi sur la protection de l'information (L.R.C. (1985), ch. O-5) :

> 19 (1) Commet une infraction quiconque, frauduleusement et sans apparence de droit, sur l'ordre d'une entité économique étrangère, en collaboration avec elle ou pour son profit et au détriment des intérêts économiques canadiens, des relations internationales ou de la défense ou de la sécurité nationales :
>
> - a) soit communique un secret industriel à une personne, à un groupe ou à une organisation;
> - b) soit obtient, retient, modifie ou détruit un secret industriel

Premièrement, la définition d'une « entité économique étrangère » est trop étroite, de sorte qu'elle omet de définir de manière exhaustive la notion de contrôle. (LaRoche, 2020) Ainsi, il devient difficile de faire la preuve qu'un lien hors de tout doute existe

[33] Voir la *Loi antiterroriste*, LC 2001, c 41

entre un accusé et une entité étrangère lors d'une accusation pour espionnage économique (LaRoche, 2020). Deuxièmement, l'élément selon lequel l'espionnage économique doit être « au détriment des intérêts économiques canadiens » est trop vague, sujet à interprétation et ultimement, pourrait faire l'objet d'un débat politique plutôt qu'un procès criminel (LaRoche, 2020). Troisièmement, comme mentionné précédemment, les entreprises sont, en général, réticentes à rapporter le vol de secrets commerciaux, pensant qu'ils perdront tôt ou tard un avantage concurrentiel et une dévaluation de leur indice boursier. LaRoche ajoute :

> firms may perceive disclosure requirements associated with prosecution as threatening the protection afforded by trade secret law. While the American EEA mandates that courts take action to preserve the confidentiality of trade secrets during EEA litigation, no such provision exists with respect to prosecutions under section 19 of the SIA. Without legal and procedural protections for trade secrets and incentives to co-operate, Canadian industry is unlikely to provide information vital to the prosecution of economic espionage (LaRoche, 2020)

Quatrièmement, les procureurs canadiens trouvent parfois plus simple, voire plus efficace de recourir à une autre disposition du Code criminel, celle de l'abus de confiance. (LaRoche, 2020) Ce faisant, il semble plus aisé pour les détenteurs de secrets commerciaux de demander réparation aux instances civiles, « par l'entremise de réclamations pour abus de confiance, manquement à une obligation fiduciaire ou rupture de contrat, en vertu d'un accord de divulgation » (LaRoche, 2020).

Similairement aux États-Unis, plusieurs ont senti le besoin de criminaliser plus fortement l'espionnage économique au Canada. C'est ce qui s'est produit le 13 mars 2020 lorsque le projet de loi C-4 (application de l'Accord Canada-États-Unis-Mexique [ACEUM]) a obtenu la sanction royale (LaRoche, 2020), et est entré en vigueur le 1er juillet 2020. À cet effet, le projet de loi C-4 est venu amender le Code Criminel, en mettant en place un cadre juridique concernant la protection et le respect des droits de propriété intellectuelle en Amérique du Nord. La section 391 du Code Criminel prévoit

désormais une définition plus précise que la section 19 de la *Loi sur la protection de l'information.* Toutefois, rien ne garantit une meilleure judiciarisation de l'espionnage économique, et plusieurs affirment que les mêmes obstacles qui s'érigent lors de poursuites judiciaires resteront (LaRoche, 2020).

3.4 L'approche étatiste par rapport à l'approche individualiste : retour sur les paradigmes dominants de l'intelligence économique

Au premier chapitre, nous avons comparé deux paradigmes dominants de l'intelligence économique, soit la guerre économique et la concurrence économique. Maintenant que nous avons survolé les rouages de l'appareil gouvernemental chinois, particulièrement les services de renseignements et les ambitions nationales de la Chine, et que nous avons dressé le portrait global de l'espionnage économique aux États-Unis et au Canada depuis les années 1990, il sera plus aisé d'appréhender les deux grands modèles socioéconomiques qui s'affrontent actuellement sur la scène mondiale.

Du côté des tenants de la guerre économique, il est davantage question de favoriser une approche étatiste, laquelle trouve son appui dans une culture qui valorise le plus souvent l'harmonie et la solidarité (T.R Reid, 1999, cité par Reid, 2016 : 823). Les tenants de la compétitivité économique priorisent plutôt des valeurs dans lesquelles l'individu occupe une place importante; la distinction et l'affirmation sont donc des traits caractériels estimés (Reid, 2016, *ibid.*). Ainsi, dans les pays où il existe une culture plus collectiviste (ou étatiste), comme en Chine, le gouvernement est davantage enclin à protéger et favoriser ses industries nationales, ainsi qu'à intervenir directement dans le marché en outillant le secteur privé d'information et de services gouvernementaux (Potter, 1998 : 56). De manière opposée, dans les pays qui préconisent une approche individualiste, comme la plupart des pays d'Occident, le rôle du gouvernement en matière d'économie est relayé au second plan, alors qu'il agit plutôt en tant que modérateur. Dans un environnement où le partage de l'information

se heurte souvent au travail en silo entre les organismes, les agences et les entreprises, le gouvernement focalise sur une meilleure transparence des entreprises et cherche, sans intervenir trop fortement, à stimuler la croissance économique nationale (Potter, 1998, *ibid.*). De ces conclusions, Melanie Reid dresse les constats suivants (Reid, 2016 : 822) :

> « Les gouvernements qui entretiennent des liens étroits avec l'industrie privée sont plus susceptibles de mener des activités d'espionnage au profit du secteur privé »
>
> « Les pays qui ont une vision nationaliste du marché mondial, et qui représentent un environnement de technologie de pointe riche en cibles pour leurs concurrents, ont tendance à avoir des lois strictes sur la protection de la propriété intellectuelle et des lois pénales précises sur l'espionnage économique »
>
> « D'autres pays qui sont tout aussi nationalistes d'un point de vue économique, mais qui ont des politiques industrielles protectionnistes minimales et des cadres juridiques déficients quant à la protection de la propriété intellectuelle, peuvent faire partie des pays qui soutiennent ou tolèrent l'espionnage économique »
>
> « Les pays développés qui ont le plus à perdre du vol de leurs secrets commerciaux et qui valorisent l'innovation (comme les États-Unis) sont évidemment en faveur d'un renforcement des peines et d'une judiciarisation plus accrue des crimes économiques »
>
> « Certains pays développés, comme le Canada et la Nouvelle-Zélande, des pays qui ont mis en place des protections juridiques similaires à l'EEA, n'ont poursuivi personne pour de tels crimes; cela pourrait suggérer qu'ils croient que de telles poursuites entravent réellement l'innovation et la productivité plutôt que de la protéger »
>
> « Des pays comme la Chine, la Russie, et l'Inde (dans une certaine mesure), vont justifier le vol de la propriété intellectuelle, car il garantit des conditions de concurrence équitables entre les pays développés et les pays émergents »

Evan H. Potter donnait le même genre d'éclairage sur le sujet en 1998 en utilisant, dans son ouvrage *Economic Intelligence & National Security*, une taxinomie des systèmes nationaux d'intelligence économique basée sur le degré de centralisation du renseignement économique (Potter, 1998 : 54-55). Dans sa méthode de classement, il expliquait que le Canada comptait à l'époque sur un réseau national d'intelligence économique hautement décentralisé : 30 services et agences du gouvernement fédéral, 128 missions diplomatiques, des bureaux provinciaux à l'étranger, ainsi qu'un environnement riche en associations relatives aux affaires nationales (ex. : la Chambre du Commerce du Canada, la Canadian Manufacturers and Exporters of Canada et le Conseil canadien des affaires) (Potter, 1998 : 55). Cette dynamique décentralisée, qui se transpose encore aujourd'hui, faisait en sorte que le Canada entretenait :

- un programme global plus défensif de collecte de renseignements économiques (axé sur la prévention de l'espionnage économique);
- un faible niveau de coopération entre le secteur public et le secteur privé;
- un faible niveau de sensibilisation quant à l'importance de l'intelligence économique dans les entreprises.

Du côté américain, les conclusions d'Evan H. Potter étaient similaires, malgré quelques nuances qui caractérisaient les États-Unis comme étant plus proactifs que le Canada dans le domaine du renseignement économique (Potter, 1998 : 54-55). Dans un environnement légèrement moins décentralisé qu'au Canada, les États-Unis offraient :

- un programme offensif de l'intelligence économique comprenant des méthodes clandestines;
- un niveau intermédiaire de coopération entre le secteur public et le secteur privé;
- un faible niveau de sensibilisation quant à l'importance de l'intelligence économique dans les entreprises.

Plus globalement, Melanie Reid fait le constat que les caractéristiques des mécanismes de protection en matière d'espionnage seraient également dues à une conception

singulière de la notion de propriété. En effet, d'un point de vue juridique, les différentes perspectives de la règle de droit expliqueraient pourquoi les États-Unis et le Canada perçoivent l'espionnage économique différemment de la Chine. Comme Melanie Reid le mentionne : « other cultures seem to view intellectual property through a different lens and are less willing to declare IP a uniquely protected right » (Reid, 2016, 822-823). Autrement dit, ce sont en partie les différences de conception de la notion de propriété et le type de gouvernance qui façonnent entre autres le cadre juridique d'un État en matière d'espionnage économique (Reid, 2016 : 823).

3.5 Conquête de marchés et prise de risques : les grandes constantes

La prise de risques et la tolérance marquée en ce qui a trait aux transferts de technologies de la part des entreprises sont d'autres caractéristiques propres à une vision compétitive de l'intelligence économique. En effet, les entreprises prennent souvent d'énormes risques sans se soucier des conséquences à plus long terme (Roper, 2014, *ibid.*). Souvent menées par l'appât du gain, plusieurs entreprises se dépêchent de conquérir des marchés sans adapter leur culture d'affaires (Katsuya, 2011), d'où cette vision plus compétitive que guerrière de l'intelligence économique, qui suppose que les dynamiques économiques se conçoivent avant tout comme un jeu. Celui-ci s'observe comme un espace de concurrence gagnant-gagnant, où la rentabilité et la performance dominent, pour l'essentiel, les objectifs des entreprises.

Par exemple, une tendance se dessine depuis plusieurs années. Certaines compagnies américaines spécialisées dans la haute technologie font des investissements précipités en RPC, lesquels comprennent des accords flous et permettent entre autres l'établissement de centres communs de R&D. En coopérant de la sorte, bien des compagnies n'ont pas connaissance du réel impact que provoque ce genre de relations d'affaires (Roper, 2014, *ibid.*). Carl Roper précise :

> The US General Accounting Office (GAO) found that US businesses have significant concerns about arbitrary licensing requirements in the PRC, because they often call for increased technology transfer. The GAO also found that transparency was the most frequent concern to be reported by US companies. Because of the lack of transparency in the PRC's laws, rules, and regulations that govern business alliances, and the dearth of accessible, understandable sources or regulatory information, US businesses suddenly find themselves being subjected to various technology transfer requirements that are never found in any written documentation or are contained in "secret" rules that only the PRC insiders know about (*Cox Report*, 1999 : 29; Roper, 2014 : 53)

Plusieurs entreprises convoitent le marché chinois et s'empressent de le conquérir avant qu'un concurrent le fasse (Roper, 2014, *ibid.*). Ce comportement entrepreneurial n'est pas étranger aux failles de la sécurité nationale américaine. Car, sans connaître véritablement les rouages du réseau industriel chinois, un grand nombre de technologies américaines peuvent rapidement se trouver entre les mains de l'appareil militaire chinois (Roper, 2014, *ibid.*; Meia Nouwens et Helena Legarda, 2018). Ce faisant, une technologie partagée avec un partenaire commercial (ex. : une coentreprise utilisée en guise de couverture) peut devenir accessible au réseau militaro-industriel de la RPC, sans que la compagnie qui fournit la technologie ne connaisse la portée d'un tel partage et les implications pour la sécurité nationale (Roper, 2014, *ibid.*).

Au Canada, les mêmes observations s'appliquent. D'ailleurs, le cas entourant la conception d'hélicoptères de combat chinois Z-10 avec la collaboration du fabricant canadien de moteurs aéronautiques Pratt & Whitney Canada (P&WC) est un exemple qui en témoigne. Depuis le milieu des années 2000, P&WC et Hamilton Sundstrand Corporation (HSC) (toutes deux filiales de la United Technologies Corporation [UTC]) ont acheminé des moteurs et des logiciels pour la conception d'hélicoptères de combat chinois. Les deux filiales ont collaboré avec la Chine en sachant qu'un embargo américain interdisait la vente d'armes à ce pays. Camouflé derrière un volet civil, le projet militaire chinois, qui laissait entrevoir des revenus annuels d'environ deux

milliards de dollars, s'est concrétisé avec les années, et ce, avec l'aide d'entreprises occidentales.

Cette histoire montre la volonté des entreprises occidentales de conquérir le marché chinois au détriment d'une culture d'affaires qui priorise une certaine prudence. Les entreprises entretiennent constamment le déni relativement aux nouvelles menaces comme le vol de propriété intellectuelle et de technologies à double usage (Katsuya et de Pierrebourg, 2010 : 22). Comme l'évoquent Michel Juneau-Katsuya et Fabrice de Pierrebourg, le fardeau de la sécurité incombe désormais aux chefs d'entreprise : « mais voilà, eux-mêmes n'étant pas sensibilisés à la question, ils ignorent ou rejettent tout bonnement la possibilité de pouvoir un jour être victimes » (Katsuya et de Pierrebourg, 2010, *ibid.*).

Ce constat observable aux États-Unis et au Canada, amène Matthew Crosston à insister sur le fait que l'adoption de « meilleures pratiques » entrepreneuriales ne se fait, en réalité que sur une base volontaire (Crosston, 2015 : 114). Cette facette socioéconomique propre aux économies plus libérales, laisse ainsi le choix aux entreprises d'adopter ou non une culture d'affaires plus sécuritaire, en rapportant, par exemple, un incident aux autorités responsables (Burstein, 2009 : 70, 989). Matthew Crosston ajoute que cette dynamique entre le secteur public et le secteur privé aux États-Unis, a longtemps été au cœur d'un dilemme : celui de renforcer le cadre légal et de faciliter le processus des poursuites judiciaires en matière d'espionnage, au détriment de la prospérité des industries nationales (Crosston, 2015 : 114-115). L'histoire a cependant montré que les politiciens américains ont constamment penché en faveur d'une prospérité optimale des entreprises et d'une faible ingérence gouvernementale, et ce, même si l'assistance du gouvernement était dans leur intérêt à plus long terme (Crosston, 2015 : 115).

3.6 Repenser les paradigmes qui guident le renseignement?

Dans un monde où la distinction des pays dépend largement de leur avance technologique et qu'en l'occurrence, les enjeux économiques se sont progressivement greffés à la juridiction de la sécurité nationale, de nombreux experts se sont posé la question à savoir si les services de renseignement devaient jouer un rôle davantage proactif dans les relations commerciales (Roper, 2014; Slate, 2009; Crosston, 2015; Katsuya et de Pierrebourg, 2010; MacOdrum, 2001). Aux États-Unis comme au Canada, plusieurs soulignent à cet effet que la frontière entre le gouvernement et le secteur privé souffre d'un manque de porosité, car plusieurs entreprises se méfient toujours d'une collaboration avec les services de renseignement dans les pratiques commerciales (Crosston, 2015 : 119; MacOdrum, 2001 : 140). Cette dynamique, comme nous l'avons vu précédemment, se distingue d'emblée des pratiques chinoises, lesquelles ne séparent pas la communauté du renseignement du monde corporatif (Slate, 2009 : 11; Manthorpe, 2019 : 8; Meia Nouwens et Helena Legarda, 2018).

Si l'espionnage économique est un enjeu difficile à circonscrire aux États-Unis (comme au Canada), c'est sans doute en raison du fait que les pistes de solutions les plus efficaces vont à l'encontre de la structure socioéconomique (individualiste) en place et des valeurs culturelles du pays (Crosston, 201, *ibid.*). En ce sens, Matthew Crosston évoque quatre éléments qui appuient la thèse selon laquelle les États-Unis ont de la difficulté à remédier à l'espionnage économique. Premièrement, les principes d'autonomie et d'autorégulation du marché viennent créer un « un profond scepticisme et une réticence » quant à l'appui du gouvernement dans les affaires commerciales (Crosston, 2015, *ibid.*). Deuxièmement, il ne semble pas y avoir un sentiment de vigilance dans les entreprises, ni les compétences nécessaires pour contrer des activités d'espionnage de plus en plus sophistiquées en provenance d'entités étrangères (Crosston, 2015, *ibid.*). Troisièmement, ce genre de dynamique socioéconomique facilite l'adoption d'une législation inefficace, vague et ambiguë pour traiter

l'espionnage économique. (Crosson, 2015, *ibid.*) Quatrièmement, une coopération entre la communauté du renseignement et les entreprises demeure un « anathème » aux bonnes pratiques commerciales, et serait même perçue comme une violation à l'éthique commerciale (Crosston, 2015, *ibid.*).

Ce dernier point amené par Matthew Crosston soulève la question suivante : les États-Unis doivent-ils éliminer la barrière qui sépare la communauté du renseignement des entreprises locales, sachant que leurs principaux adversaires politiques l'ont déjà fait? Autrement dit, pour assurer un perpétuel coup d'avance sur ses concurrents et détenir un avantage concurrentiel à leurs dépens, est-ce que les États développés doivent brouiller la ligne entre la sécurité et l'économie, sachant que les puissances économiques sont de plus en plus influentes dans les rivalités politiques et militaires? Pour Roger George, toutefois, le paradigme traditionnel du renseignement occidental, utile pour traiter principalement des menaces à caractère étatique, n'est plus aussi efficace aujourd'hui (Cité par Slate, 2009 : 9). Comme l'estime William J. Lahneman, les phénomènes globaux et transnationaux auxquels sont désormais confrontés les services de renseignement, forcent ces derniers à opter pour une nouvelle approche qui deviendrait à la fois plus inclusive et plus flexible (Lahneman, 2010 : 209).

Pendant plusieurs années, l'appareil de sécurité nationale américain n'a pas considéré l'acquisition de technologies par la Chine comme une priorité du renseignement (Slate, 2009 : 10). Selon Robert Slate, la communauté du renseignement n'a pas établi rapidement des exigences en matière de collecte de renseignement sur le gouvernement chinois, notamment en ce qui a trait aux efforts commerciaux visant l'acquisition d'entreprises américaines, au repérage et à l'obtention des progrès technologiques américains, ainsi qu'aux relations d'affaires impliquant la Chine et les entreprises américaines de haute technologie (Slate, 2009, *ibid.*). Les services de contre-espionnage aux États-Unis ne se sont pas adaptés assez rapidement pour contrer l'espionnage économique chinois (Slate, 2009, *ibid.*) et le vol de propriété intellectuelle a longtemps été perçu comme un problème qui n'impliquait pas directement les enjeux

de sécurité nationale (Slate, 2009, *ibid.*). De ce fait, comme le soutient Robert Slate, « […] IP would be treated primarily as an economic, legal, and trade-related matter » (Slate, 2009, *ibid.*).

Un changement de paradigme ou de perception du renseignement qui ferait de l'intelligence économique un état d'esprit dont les pratiques dominantes seraient davantage axées sur la contre-ingérence, la sensibilisation, la prévention et la protection (Bulinge et Moinet, 2013 : 58) bousculeraient sans doute les grands modèles socioéconomiques en place. Ces derniers se dressent incontestablement en obstacles lorsque vient le temps de mettre en pratique des mesures visant à contrer efficacement l'espionnage économique (Crosston, 2015 : 120). Il est ainsi souvent question de méfiance à l'égard des services de renseignement, de manque de transparence des entreprises et des autorités gouvernementales, d'opposition entre les secteurs public et privé, de non-ingérence du gouvernement dans les affaires économiques, etc. Pendant ce temps, les opérations d'espionnage économique prennent de plus en plus d'ampleur à l'échelle mondiale (Crosston, 2015, *ibid.*). La nécessité de s'interroger sur les intérêts nationaux devient, somme toute pour plusieurs, de plus en plus pressante.

CONCLUSION

L'intensification de l'espionnage économique chinois aux États-Unis et au Canada est en partie la résultante d'une conception singulière de l'intelligence économique largement différente de celle de la Chine. Comme nous l'avons vu, la Chine compte sur un programme d'intelligence économique largement plus inclusif que ceux des États-Unis et du Canada. Le renseignement occupe, en ce sens, une place prépondérante; il prête directement assistance au monde entrepreneurial, diplomatique, universitaire et médiatique, dans le but de servir les ambitions nationales du PCC. Alors que les secteurs/partenariats publics-privés et militaires-civils ne sont pas séparés les uns des autres en Chine, aux États-Unis et au Canada, la vision de l'économie ne permet pas ce genre d'association. La posture stratégique adoptée par les deux blocs idéologiques renferme d'un côté des aspects beaucoup plus patriotiques, protectionnistes et subversifs, alors que de l'autre, le risque, la performance, la rentabilité et l'opportunité qualifient davantage le paradigme dominant.

Comme l'ont indiqué Frank Bulinge et Nicolas Moinet, un État dont le paradigme dominant en intelligence économique est la « guerre économique », teinte principalement sa grille d'analyse par la géoéconomie, la géostratégie et la polémologie (Bulinge et Moinet, 2013 : 57). En revanche, les États dont le paradigme de la compétitivité économique guide leur vision des relations économiques verront la conquête de marché comme principal objet ontologique (Bulinge et Moinet, 2013 : 59). De ces deux visions distinctes découlent des pratiques singulières. Pour les tenants de la guerre économique, l'espionnage, la propagande et la déstabilisation figurent parmi les activités les plus observables (Bulinge et Moinet, 2013 : 57). *A contrario*, les tenants de la compétitivité économique se concentrent essentiellement sur la veille technologique, le lobbying et le *benchmarking* (Bulinge et Moinet, 2013 : 59). L'aspect

sécuritaire de ce modèle est souvent relayé au second plan, pour laisser place à l'opportunisme.

Comme l'a montré ce mémoire, l'espionnage économique chinois aux États-Unis et au Canada est une menace qui fragilise les deux pays depuis plusieurs décennies. Parce que les États-Unis et le Canada sont des États basés sur le savoir, ils investissent massivement dans la R&D et ont des centres de recherche à la fine pointe de la technologie. Ceux-ci font l'objet de convoitise de pays comme la Chine dont les ambitions nationales la pressent de détenir rapidement un avantage concurrentiel sur ses rivaux. En court-circuitant les processus onéreux de R&D, la Chine s'adonne fréquemment au vol de propriété intellectuelle, ainsi qu'à la collecte d'information, par l'entremise de divers canaux informationnels (journalistes, étudiants, ingénieurs, scientifiques, hommes d'affaires, etc.).

Le ciblage de données sensibles détenues par les firmes et les gouvernements américain et canadien, engendre des pertes annuelles qui se comptent, depuis plusieurs années, par centaines de milliards de dollars. Des chiffres qui demeurent somme toute peu précis et rarement évoqués, notamment au Canada. Motivées par l'appât du gain, précisément par la conquête du marché chinois, les entreprises américaines et canadiennes tardent à revoir leur modèle d'affaires. Au même titre, les services de contre-espionnage aux États-Unis et au Canada ont pris un certain temps à faire du vol de propriété intellectuelle une priorité en matière de sécurité nationale. Guidés longtemps par un modèle de renseignement statocentré, et amputés par les nombreuses coupures budgétaires entraînées par les évènements du 11 septembre, les services du contre-espionnage ont, par conséquent, tardé à revoir rapidement leur approche pour appréhender plus efficacement les nouvelles menaces de nature géoéconomique.

Dès lors, les services de contre-espionnage américains et canadiens ont été, et sont toujours aux prises avec un problème bien plus profond qu'on pourrait le penser. L'espionnage économique n'illustre pas uniquement le vol d'information entre États,

mais également un fléau qui place dorénavant les entreprises sur la ligne de front des tensions géoéconomiques. Espionnage, sabotage, cyberattaques, les moyens ne manquent pas : la ligne de front n'est plus tracée entre deux États, désormais, elle semble être tracée partout. Dans le contexte actuel, deux grands modèles, labellisés par la guerre commerciale sino-américaine, se redessinent à l'horizon. Ces modèles semblent dorénavant plus de nature économique qu'idéologique. L'environnement mondial hyperconcurrentiel laisse désormais entrevoir un monde mené par une fervente course à l'innovation technologique, où les gains nationaux (re)deviennent la plus importante prérogative pour les superpuissances de la planète.

BIBLIOGRAPHIE

18 U.S. Code § 1831.Economic espionage. *Legal Information Institute*. *Cornell Law School*. (Consulté le 3 novembre 2020) https://www.law.cornell.edu/uscode/text/18/1831

Alloing, Camille et Nicolas Moinet. (2016). « Les signaux faibles : du mythe à la mystification ». *Hermès, La Revue*, 3(76): p. 86 -92.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage (2008). *Office of National Counterintelligence Executive*. (Consulté le 4 novembre 2020) https://apps.dtic.mil/dtic/tr/fulltext/u2/a506093.pdf

Annual Report to Congress. (2019). « Military and Security Developments Involving the People's Republic of China 2019 ». *Office of the Secretary of Defense*. 123 pages. (Consulté le 3 novembre 2020) http://www.andrewerickson.com/wp-content/uploads/2019/05/DoD_China-Report_2019.pdf

B20 Summit, Hangzhou. (2016). « A New Starting Point for China's Development: « A New Blueprint for Global Growth ». *G20 Research Group*, University of Toronto. (Consulté le 3 novembre 2020). http://www.g20.utoronto.ca/2016/160903-xi.html

Barton, Rosmary. (2014). « Chinese cyberattack hits Canada's National Research Council » *CBC News*. (Consulté le 17 janvier 2021) https://www.cbc.ca/news/politics/chinese-cyberattack-hits-canada-s-national-research-council-1.2721241

Blackwell, Tom. (2019). « U.S. seeks to extradite McGill professor accused of conspiring to send technology to China ». *National Post*. (Consulté le 17 janvier 2021) https://nationalpost.com/news/u-s-seeks-to-extradite-mcgill-professor-accused-of-conspiring-to-send-technology-to-china

Broad, William J. (2020). « China Reports Progress in Ultra-Secure Satellite Transmission » *New York Times*. (Consulté le 3 novembre 2020). https://www.nytimes.com/2020/06/15/science/quantum-satellites-china-spying.html

Bronskill. Jim. (2014). « La cyberattaque au CNRC a touché un système de données personnelles ». *La Presse*. (Consulté le 17 janvier 2021) https://www.lapresse.ca/actualites/national/201407/31/01-4788308-la-cyberattaque-au-cnrc-a-

touche-un-systeme-de-donnees-personnelles.php?utm_categorieinterne=trafficdrivers&utm_contenuinterne=cyberpresse_lire_aussi_4329787_article_POS3

Cidon, Asaf. (2015) « La protection de la propriété intellectuelle dans le nuage ». *Organisation mondiale de la propriété intellectuelle (OMPI)*. (Consulté le 3 novembre 2020).https://www.wipo.int/wipo_magazine/fr/2015/03/article0004.html

Coats, Daniel R. (2019). « Worldwide Threat Assessment of the US Intelligence Community ». *Senate Select Committee on Intelligence*. 42 pages. (Consulté le 3 novembre 2020). https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf

Colin, LaRoche. (2020). « A new way to prosecute Economic Espionage? Section 19 of the Security of Information Act, and the new "Trade Secrets" Offence ». *Intrepid* (Consulté le 12 janvier 2021) A new way to prosecute Economic Espionage? Section 19 of the Security of Information Act, and the new "Trade Secrets" Offence — INTREPID (intrepidpodcast.com)

CTIC Limited. Site Web sous l'onglet : « Company ». (Consulté le 3 novembre 2020) https://web.archive.org/web/20120624034913/http:/www.citic.com/wps/portal/enlimited/gyzx/gsjs

Decloquement, Franck. (2014). « Espionnage et intelligence économique ». *ActuEntreprise*. (Consulté le 3 novembre 2020). https://www.actuentreprise.com/?s=franck+decloquement&x=0&y=0

Department of Justice. (2020). « Singaporean National Pleads Guilty to Acting in the United States as an Illegal Agent of Chinese Intelligence », *Office of Public Affairs*. National Security Division (NSD), USAO - District of Columbia. (Consulté le 3 novembre 2020) https://www.justice.gov/opa/pr/singaporean-national-pleads-guilty-acting-united-states-illegal-agent-chinese-intelligence

Elsa B. Kania et John Costello (2018). « Quantum Hegemony? China's Ambitions and the Challenge to U.S. Innovation Leadership ». *Center for New American Security*, 47 pages. (Consulté e 3 novembre 2020). https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/CNASReport-Quantum-Tech_FINAL.pdf?mtime=20180912133406&focal=none

Federal Bureau Investigation. (2010). « Former Boeing Engineer Sentenced to Nearly 16 Years in Prison for Stealing Aerospace Secrets for China ». *Communiqué de presse*, Division de Los Angeles (Consulté le 17 janvier 2021) https://archives.fbi.gov/archives/losangeles/press-releases/2010/la020810.htm

Federal Bureau Investigation. (2013). « Former Employee of New Jersey Defense Contractor Sentenced to 70 Months in Prison for Exporting Sensitive Military Technology to China ». *Communiqué de presse*, Division du New Jersey. (Consulté le 17 janvier 2021) https://archives.fbi.gov/archives/newark/press-releases/2013/former-employee-of-new-jersey-defense-contractor-sentenced-to-70-months-in-prison-for-exporting-sensitive-military-technology-to-china

IP Commission Report. (2013). « The Report of The Commission on The Theft of American Intellectual Property ». *The National Bureau of Asian Research*. 89 pages. (Consulté le 4 novembre 2020) https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report.pdf

IP Commission Report. (2017). « The Theft of American Intellectual Property: Reassessments of The Challenge and United States Policy ». *The National Bureau of Asian Research*. 24 pages. (Consulté le 3 novembre 2020) https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf

Jing, Meng. (2018). « Is Xi Jinping's iron grip better than Adam Smith's invisible hand for technology innovation? ». *South China Morning Post*. (Consulté le 3novembre 2020). https://www.scmp.com/tech/article/2173128/xi-jinpings-iron-grip-better-adam-smiths-invisible-hand-technology-innovation

Joint Strategic Plan on Intellectual Property Enforcement. (2010). *Executive Office of the President*. (Consulté le 4 novembre 2020) https://www.hsdl.org/?abstract&did=22983

Joske, Alex. (2020). « Hunting the Phoenix ». Australian Strategic Policy Institute. (Consulté le 11 mai 2021). https://www.aspi.org.au/report/hunting-phoenix

Juillet, Alain. (2011). « Cessons d'être naïfs », *Les Échos*, (Consulté le 3 novembre 2020). https://www.lesechos.fr/2011/01/cessons-detre-naifs-1088638

Juillet, Alain. (2012). « Le renseignement et son évolution compétitive ». *Défense nationale*, Revue n° 755 : p. 26-30. (Consulté le 3 novembre 2020). https://www.defnat.com/e-RDN/vue-article.php?carticle=15744

Juillet, Alain. (2014). « La sécurité numérique, c'est avant tout un état d'esprit. » *Préventica*. (Consulté le 3 novembre 2020). https://www.preventica.com/actu-interview-juillet-cdse.php

Juillet, Alain. (2019). Intervention à la conférence : « La veille stratégique et l'intelligence économique ». *Association Tunisienne de Veille et*

d'intelligence Compétitive. (Consulté le 3 novembre 2020). https://www.atvic.tn/?s=Alain+juillet

Juillet, Alain. (2020). « Espionnage économique : la France peut-elle faire face? » *RT France*, (Consulté le 3 novembre 2020). https://francais.rt.com/recherche?q=la+source+alain+juillet+&df=&dt=&type

Katsuya, Michel-Juneau. (2019). « Menaces en cybersécurité - Exploration des différents types de menaces », *Cybersécurité 20/20*. (Consulté le 3 novembre 2020) https://hub.novipro.com/fr/menaces-exploration-des-diff%C3%A9rents-types-de-menaces

Kennedy, Scott. (2015). « Made in China 2025 ». *Center for Strategic & International Studies*. (Consulté le 3 novembre 2020). https://www.csis.org/analysis/made-china-2025

Laïdi, Ali. 2016. « 26 - Les armes de la guerre économique contemporaine ». In *Histoire mondiale de la guerre économique*, Hors collection, Paris: Perrin, 437-50. https://www.cairn.info/histoire-mondiale-de-la-guerre-economique--9782262069285-p-437.htm.

Lamigeon, Vincent. (2013) « La vérité sur... les transferts industriels à la Chine ». *Challenges*. (Consulté le 3 novembre 2020). https://www.challenges.fr/entreprise/la-verite-sur-les-transferts-industriels-a-la-chine_225653

Larouche, Vincent. (2020). « Le Canada, base de lancement pour espions chinois ». *La Presse*. (Consulté le 17 janvier 2021) https://www.lapresse.ca/actualites/2020-01-26/le-canada-base-de-lancement-pour-espions-chinois

Matthew Johnson, « Annual Study of Intangible Asset Market Value» from *Ocean Tomo, LLC, Intellectual Capital Equity*, 22 septembre 2020 (https://www.oceantomo.com/insights/ocean-tomo-releases-intangible-asset-market-value-study-interim-results-for-2020/)

Mitrovica, Andrew et Jeff Sallot. (2000). « China set up crime web in Canada, report says ». *The Globe and Mail*. (Consulté le 3 novembre 2020) https://www.theglobeandmail.com/news/national/china-set-up-crime-web-in-canada-report-says/article4163320/

Nouwens, Meia et Helena Legarda. (2018) « China's pursuit of advanced dual-use technologies ». *International Institute for Strategic Studies*. (Consulté le 3 novembre 2020) China's pursuit of dual-use technologies (iiss.org)

Overseas Security Advisory Council. « A Cooperative Partnership ». *U.S Department of State*. (Consulté le 3 novembre 2020) https://www.osac.gov/About/WhoWeAre

Podsywalow, Michael. (2012). « Preventing Corporate Espionage ». *Risk Management*. (Consulté le 4 novembre 2020) http://www.rmmagazine.com/2012/03/01/preventing-corporate-espionage/

Ponniah, Kevin. (2020). « How a Chinese agent used LinkedIn to hunt for targets », *BBC News*. (Consulté le 3 novembre 2020) https://www.bbc.com/news/world-asia-53544505

Rapport du Club informatique des grandes entreprises françaises (CIGREF). (2003). « Intelligence économique et stratégique : les systèmes d'information au cœur de la démarche ». 131 pages (Consulté le 3 novembre 2020). https://www.cigref.fr/cigref_publications/RapportsContainer/Parus2003/2003_-_Intelligence_Economique_Strategique_web.pdf

Rapport du Comité de surveillance des activités de renseignement de sécurité (CSARS) (1999-2000). « Recommandations et principales constatations ». (Consulté le 3 novembre 2020) https://www.canada.ca/fr/surveillance-activites-renseignement-securite/organisation/rapports-annuels/rapport-annuel-1999-2000/recommandations-principales-constatations-rapport-annuel-1999-2000.html

Rapport du National Counterintelligence and Security Center. (2018). « Foreign Economic Espionage in Cyberspace ». *Office of The Director of National Intelligence*. 15 pages. (Consulté le 4 novembre 2020) https://www.dni.gov/index.php/ncsc-newsroom/item/1889-2018-foreign-economic-espionage-in-cyberspace

Rapport du Web Economic Forum. (2015). « Geo-economics Seven Challenges to Globalization ». *Web Economic Forum*. (Consulté le 3 novembre 2020). http://www3.weforum.org/docs/WEF_Geoeconomics_7_Challenges_Globalization_2015_report.pdf

Rapport Sidewinder. (1997). « Chinese Intelligence Services and Triads Financial Links in Canada ». *Gendarmerie royale du Canada et Service du renseignement de sécurité*. 23 pages. (Consulté le 3 novembre 2020) https://www.primetimecrime.com/Articles/RobertRead/sidewinder.pdf

Reportage ARTE. (2016). « Le dragon à mille têtes ». *ARTE*. (Consulté le 3 novembre 2020). https://info.arte.tv/fr/le-dragon-mille-tetes-le-film

Rogin, Josh. (2012). « NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history ». *Foreign Policy*. (Consulté le 3 novembre 2020). https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/

Statistica. (2020). « Study field distribution of Chinese students in the United States in academic year 2018/19 ». (Consulté le 3 novembre 2020) https://www.statista.com/statistics/372909/chinese-students-in-the-us-by-subject/

Strategic Direction. (2012). « Tales from the front line of corporate espionage » 28(9): p. 29-32. (Consulté le 3 novembre 2020). https://www.emerald.com/insight/content/doi/10.1108/02580541211256530/full/html

Turenne, Martine. (2011). « Les entreprises sont naïves et innocentes face à l'espionnage ». *Les Affaires*. (Consulté le 3 novembre 2020) https://www.lesaffaires.com/techno/technologie-de-l-information/-les-entreprises-sont-naives-et-innocentes-face-a-l-espionnage-/523406

United States Department of Justice. (2014). « Walter Liew Sentenced to Fifteen Years in Prison for Economic Espionage ». *The United Sates Attoney’s Office*, District de Californie. (Consulté le 17 janvier 2021) https://www.justice.gov/usao-ndca/pr/walter-liew-sentenced-fifteen-years-prison-economic-espionage

United States Department of Justice. (2015). «Chinese Professors Among Six Defendants Charged with Economic Espionage and Theft of Trade Secrets for Benefit of People’s Republic of China » *Office of Public Affais*. (Consulté le 17 janvier 2021) https://www.justice.gov/opa/pr/chinese-professors-among-six-defendants-charged-economic-espionage-and-theft-trade-secrets

United States Department of Justice. (2018). « Chinese National Allegedly Exported Devices with Military Applications to China ». *District du Massachusetts*. (Consulté le 17 janvier 2021) https://www.justice.gov/usao-ma/pr/chinese-national-allegedly-exported-devices-military-applications-china

United States Department of Justice. (2018). « Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information ». *Office of Public Affairs*. (Consulté le 17 janvier 2021) https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion

Vachon, Louis et Frédérick Gagnon. (2020). « Le Canada sous le feu croisé des conflits géoéconomiques ». *La Presse*. (Consulté le 3 novembre 2020) https://www.lapresse.ca/debats/opinions/2020-07-12/le-canada-sous-le-feu-croise-des-conflits-geoeconomiques.php

Waguespack, Michael J. (2001). Témoignage sur le programme ANSIR. *The House Committee on Government Reform, Subcommittee on National Security, Veterans Affairs, and International Relations.* Washington, DC. (Consulté le 3 novembre 2020) https://archives.fbi.gov/archives/news/testimony/fbis-ansir-program

Wray, Christopher. (2020). « The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States ». *Hudson Institute*. (Consulté le 3 novembre 2020) https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states