Chaire Renseignement

Étude
Juin 2026

La France face à l'ingérence économique : l'impérieuse nécessité d'une stratégie nationale de souveraineté et de sécurité économiques

Didier Gros

Sous la direction du professeur Walter Bruyère-Ostells

« [...] les plus forts tirent tout le parti possible de leur puissance, tandis que les plus faibles n'ont qu'à s'incliner. » [1]

1. Thucydide, « La Guerre du Péloponnèse », traduction de Denis Roussel, Éditions Gallimard, folio classique, 1964, Livre V, Chapitre VII, p. 439

sciencespo.aix

Table des matières

Résumé

Les ingérences ou tentatives d'ingérence économiques frappent la France au quotidien. Sur fond de bouleversement géopolitique et d'accroissement des tensions en tous domaines, la compétition économique se fait chaque jour davantage agressive, dans ses buts comme dans ses modalités.

La sécurité économique est donc à l'ordre du jour. Certes, le concept fait toujours l'objet de débat. Nous considérons toutefois, à l'instar d'ailleurs de nos principaux partenaires-concurrents ou adversaires, Etats-Unis et Chine en particulier, qu'il est pertinent, à deux conditions : qu'il soit compris comme étant indissociable du concept de sécurité nationale, donc consubstantiel à celui de souveraineté nationale d'une part ; et qu'il soit d'autre part appréhendé de manière holistique, comme un champ d'action où les acteurs concernés agissent de manière réactive et proactive pour protéger et promouvoir des intérêts stratégiques assumés.

Le phénomène d'ingérence revêt plusieurs formes catégorisées comme autant de menaces à l'aide de la typologie suivante : capitalistique, physique, humaine, réputationnelle, cyber et juridique (*lawfare*). Face à ce défi longtemps sous-estimé malgré de nombreuses mises en garde, ce dès les années 90, la France a progressivement renforcé ses dispositifs de protection et s'est dotée en 2019 d'une politique publique de sécurité économique, assortie d'un arsenal de lois, règlementations et autres dispositions organisationnelles.

Aujourd'hui, l'administration, de l'Élysée aux ministères en passant par les services de renseignement (SR) réorganisés en conséquence, s'implique résolument. Les entreprises, principalement les grands groupes, se mobilisent davantage, et le milieu académique et des experts, notamment en matière d'intelligence économique, fait de même. Pour autant, malgré les efforts entrepris et les progrès réalisés, une analyse critique des mesures prises ces dernières années laisse transparaître des failles et des insuffisances. Le constat, quasi unanime, est celui d'une France encore timorée, juxtaposant les entités, règlements, procédures et mesures divers, culturellement réticente aux efforts d'adaptation pourtant indispensables à fournir et, surtout, handicapée par l'absence d'une véritable direction politico-stratégique. A la question fondamentale : « que veut la France en matière de souveraineté et de sécurité économiques ? », la réponse est confuse, incertaine voire inexistante. Or, le défi est bien trop systémique pour être relevé par une simple collection d'actions ou de dispositions, qui plus est essentiellement défensives, dans un périmètre mal défini, et sans structure de pilotage fédératrice s'appuyant sur l'ensemble des acteurs concernés.

Nous estimons dès lors que l'élaboration et la mise en œuvre d'une stratégie nationale, à l'intersection du politique et de l'opérationnel, est un impératif. Celle-ci doit se construire à partir d'une vision (que veut-on pour la France à moyen et à long terme sur le plan économique, ce qui implique la définition d'une politique économique ou, a minima, d'une politique industrielle) et autour d'intérêts et de grands objectifs stratégiques déclinés par filières et secteurs. Elle doit également se matérialiser par l'établissement d'une structure centrale, sous la forme d'un état-major doté de pouvoirs décisionnaires, chargée de définir, orienter, conduire et évaluer l'ensemble des stratégies secondaires et plans d'action associés.

C'est pourquoi cette étude propose, à titre illustratif, un canevas de réflexions et un modèle sommaire de stratégie, assortis d'un ensemble de recommandations concourantes thématisées et problématisées (s'organiser ; connaître, anticiper et influencer ; former et sensibiliser ; s'adapter et innover ; évaluer et sanctionner ; faire savoir), dont nous pensons que la mise en œuvre pourrait utilement contribuer à renforcer l'écosystème national.

Il nous faut voir le monde tel qu'il est et accepter de penser la conflictualité qui le sous-tend et le façonne. Il n'y a de stratégie possible que dans le cadre de la puissance assumée, entendue comme conjonction d'une volonté, de capacités et d'une politique d'influence. Il faut, pour la porter, qu'émerge enfin une « équipe France » décidée à tracer sa voie face à l'adversité.

Remarques liminaires

Nature de l'étude

Cette étude a pour point de départ les séminaires organisés de 2023 à 2025 par la Chaire Renseignement de l'IEP d'Aix-en-Provence sur la problématique de l'ingérence économique en France[2]. Elle sert deux objectifs :

- Établir une synthèse des séminaires qui puisse servir de base à des enseignements ou à des travaux ultérieurs, et être accessible au « grand public » ;
- Approfondir certains constats effectués ou réflexions partagées dans le but d'émettre des recommandations à l'attention d'un public ciblé.

Pour ce faire, nous nous sommes tout d'abord appuyés sur les séminaires et les propos de « grands témoins », sur la consultation de nombreux rapports et auditions parlementaires ainsi que sur la littérature scientifique afférente. Nous avons complété ce travail par trente-deux entretiens conduits au sein de l'administration centrale ou territoriale, incluant quatre services de renseignement du premier cercle, avec différents acteurs du monde de l'entreprise (grands groupes, PME, start-ups), ainsi qu'avec des experts des milieux privés ou académiques spécialisés en sécurité économique et intelligence économique (IE)[3].

L'étude traite en particulier de la question de l'ingérence économique dans le contexte de la compétition stratégique internationale dont on mesure chaque jour la nature de plus en plus agressive et désinhibée, au point que certains experts reconnus n'hésitent pas à parler de « guerre économique »[4]. Par le prisme des ingérences sont ainsi étudiées les actions de quelques « partenaires-concurrents »[5], les Etats-Unis et la Chine d'une part, d'acteurs européens (Allemagne et Italie) et de certains partenaires du Proche et Moyen-Orient (PMO), les pétromonarchies et Israël notamment, d'autre part. Un focus est appliqué sur l'action des services de renseignement de certains de ces pays, et par conséquent sur l'action de nos propres services. Sont également abordées les questions de sécurité et d'intelligence économiques dont les définitions et périmètres demeurent l'objet de controverses d'experts, et que l'on s'applique ici à éclaircir.

Nous tenons enfin à préciser que certaines informations consultées ou obtenues au cours des entretiens, bien que non classifiées, sont de nature confidentielle et ne peuvent donc être citées ou attribuées ouvertement.

L'enjeu conceptuel et définitionnel

L'enjeu conceptuel et définitionnel ne peut être négligé lorsque l'on aborde la question des ingérences étrangères en matière économique.

---

[2] Il s'agit des séminaires suivants : « Les entreprises françaises face aux services de renseignement chinois », Aix-en-Provence, 6 juillet 2023 ; « Les entreprises françaises face aux services de renseignement américains », Aix-en-Provence, 20 septembre 2024 ; « Les entreprises françaises face aux services de renseignement étrangers », en collaboration avec le Cabinet Gide, Paris, 28 janvier 2025.

[3] Voir Annexe 1 – Entretiens.

[4] M. Christian Harbulot, fondateur de l'École de guerre économique (EGE) et du CR 451, défend cette thèse.

[5] Cette expression est notamment utilisée par Mme Berthon, DGSI, dans : Anne Drif et David Barroux, « Les modes opératoires de l'espionnage économique sont tellement variés et pernicieux... » : l'alarme de la patronne de la DGSI », *Les Échos*, 31 octobre 2025.

Il porte d'abord sur la notion d'ingérence elle-même, qui pose la question de la compréhension de la nature du contexte (« guerre économique » ou compétition stratégique entre « partenaires-concurrents »), et sur la distinction entre ingérence et influence.

Il concerne également le périmètre du « champ conflictuel ». Doit-on prendre en compte l'ensemble de la fonction économie ou seulement les secteurs ou filières dits stratégiques ?

Et enfin, il comprend les buts à atteindre et la nature des actions à mener dans le cadre défini. S'agit-il de souveraineté, d'autonomie voire d'indépendance dans certains secteurs ? Les modalités à mettre en œuvre, soit les voies et moyens, doivent-elles privilégier l'offensive ou la défensive, le proactif ou le réactif ?

Ces interrogations s'inscrivent dans le contexte plus large du concept de sécurité économique. Sur ce sujet, plusieurs écoles s'affrontent en France sans parvenir à un consensus. Ainsi, les uns estiment que le concept de sécurité économique sur lequel repose l'écosystème français est inadapté car essentiellement défensif, tandis que d'autres soulignent que les Etats-Unis comme la Chine, qui déploient des méthodes extrêmement agressives tout en exerçant une influence dont on mesure chaque jour les effets, s'appuient pourtant sur ce concept prétendument défensif. D'autres encore encouragent le développement de l'intelligence économique conçue comme une approche holistique à visée offensive et d'influence sur fond de dispute quant à sa nature et son périmètre, comme l'indique d'ailleurs en toute franchise la non-définition proposée par le rapport Lienemann-Lemoyne de 2023[6]. Or, compartimenter sécurité économique et intelligence économique nous paraît stérile. Nous estimons en effet que la sécurité économique est fondamentalement attachée au concept de souveraineté nationale et ne saurait alors se réduire à un arsenal de mesures de protection pensées dans le cadre d'une vision réductrice et, somme toute, inopérante sur le plan stratégique et non pertinente dans l'écosystème international actuel. Bien au contraire, elle doit être comprise comme un tout indissociable d'une grande stratégie qui ne peut s'appréhender que dans le cadre encore plus large de la sécurité nationale. En ce sens, la sécurité économique est une composante majeure de la sécurité nationale. Elle dépasse la logique binaire attaque-défense, d'ailleurs mal adaptée au monde économique, et se déploie sous la forme de différentes stratégies combinant actions et réactions, renseignement et influence. Aujourd'hui plus encore qu'hier, il faut maîtriser l'information, sa collecte, son traitement et son exploitation selon une logique manœuvrière qui permette d'œuvrer à la consolidation de la souveraineté nationale.

Ce qu'est – et n'est pas – une stratégie

Comme nous le verrons plus en détail (*cf.* Partie 2), la France dispose d'un arsenal assez complet, en voie d'étoffement qui plus est, en matière de « protection économique ». Elle possède également un certain nombre de capacités et de compétences en matière d'intelligence économique pour agir de manière plus proactive. Cependant, lui fait défaut sans doute l'essentiel : la direction politico-stratégique, comprise comme la mise en cohérence, sur le fond et sur la forme, d'une vision, d'une politique économique et industrielle, et d'un ensemble de voies et moyens pour atteindre les objectifs de nature stratégique fixés. La posture de la France est fondamentalement défensive et ne se nourrit pas assez de politiques pensées, périmétrées et déployées au regard du contexte actuel et des perspectives plausibles à moyen terme, et au-delà. Sur quelle politique économique nationale s'appuie-t-on ? Sur quelle politique industrielle, à l'heure où nous ne cessons de parler de

[6] Sénateurs Marie-Noëlle Lienemann et Jean-Baptiste Lemoyne, *Anticiper, adapter, influencer : l'intelligence économique comme outil de reconquête de notre souveraineté*, Rapport d'information n° 872 (2022-2023), déposé le 12 juillet 2023.

réindustrialisation ? Quelles sont nos priorités pour aujourd'hui et après-demain, secteur par secteur ? Mesurons-nous vraiment nos atouts comme nos limites et vulnérabilités, et en tirons-nous des enseignements pour informer une stratégie nationale en la matière ?

Car il nous faut parler de stratégie. Ce terme est galvaudé, et peu en comprennent la véritable signification ou la portée. L'idée de la mise en place d'une stratégie est régulièrement évoquée, à juste titre, mais rarement explicitée et précisée, hormis dans les cercles spécialisés. Or, sa seule évocation ne résout rien et ne sert qu'à se donner bonne conscience ou à faire impression. Car une stratégie est bien plus qu'un plan d'action. Il s'agit d'un processus à la fois complexe (une stratégie suppose l'itération, est dynamique et inscrite dans la durée) et rigoureux (méthode et détermination sont requises). Plus encore, penser stratégie, c'est tout d'abord penser conflictualité. La stratégie implique l'opposition, la dialectique, l'affrontement des volontés et des capacités. Le contexte international actuel, d'essence conflictuelle, s'y prête ! Une stratégie se conçoit et se conduit en outre à l'intersection du politique et de l'opérationnel, et doit constituer un ensemble cohérent qui repose sur des structures et des fonctions, sur des voies et des moyens (pouvant constituer une doctrine), au service d'une vision, d'un état final recherché et, surtout, d'intérêts nationaux assumés. Ce dernier point est en effet crucial et justifie à lui seul la nécessité d'une stratégie nationale car se poser la question des intérêts enclenche un processus aussi vertueux qu'introspectif qui force le courage politique et suscite la mobilisation opérationnelle.

Dès lors, pour la France, postuler que nous ne faisons face qu'à des « partenaires-concurrents » et non pas à des adversaires éventuellement animés d'intentions hostiles, fussent-ils alliés, préempte la possibilité même d'une stratégie puisque la vision politique ainsi affirmée rejette la confrontation et la conflictualité. On pourra débattre du recours au terme de « guerre », certes, mais on s'étonnera aussi du fait que les vocables « lutte » et « combat » soient dans la bouche de l'ensemble de la classe politique au quotidien et continuent pourtant de heurter les consciences en matière de « compétition économique ». Car les faits sont têtus, pourtant : dans ce domaine, il s'agit bien de rapports conflictuels, il s'agit bien de dialectique, il s'agit bien d'affrontement des volontés et des capacités. Ne pas l'accepter, c'est renoncer à la stratégie, c'est donc s'interdire la cohérence, la pertinence et l'efficacité.

Introduction

En première section du mémorandum présidentiel intitulé « *America First Investment Policy* », signé par Donald J. Trump le 21 février 2025, est placée la formule suivante : « *Economic security is national security* ».[7] Peut-on être plus explicite ? Dans les faits, depuis le milieu des années 2010, Washington porte une vision de plus en plus englobante du concept de sécurité nationale qui légitime les mesures les plus extrêmes, mâtinées de bienveillants discours ou tout simplement brutalement assumées, allant du protectionnisme d'État à la prédation, à l'encontre des alliés comme des adversaires. De son côté, la Chine a formalisé dès 2014 le concept de « sécurité nationale globale »[8] dont la logique expansive, bien qu'elle s'en défende, conduit à une politique de « sécurisation de tout »[9] et fait de la sécurité économique la « base »[10] de ses efforts en soutien de sa « sécurité politique » (préservation du régime).

Prise dans l'étau de la rivalité systémique sino-américaine qui tend chaque jour davantage à structurer les rapports de force globaux, l'Union européenne s'emploie à tracer sa voie, mais peine à convaincre. Certes, on relèvera qu'elle s'est dotée en 2023 d'une stratégie de sécurité économique[11], très récemment complétée et renforcée, témoignant ainsi qu'elle n'ignore pas la criticité des enjeux associés aux évolutions paradigmatiques du contexte international en matière de compétition économique[12]. Toutefois, le 16 septembre dernier, M. Draghi, peinant à masquer son exaspération face à une Union qu'il juge malgré tout léthargique, la rappelait une énième fois à ses responsabilités en ces termes : « *À l'époque, des inquiétudes avaient été exprimées concernant le nationalisme économique, le protectionnisme et le risque que l'Europe abandonne un ordre mondial fondé sur des règles. Mais l'année écoulée a clairement montré que nous évoluons dans un monde différent. La frontière entre économie et sécurité est de plus en plus floue. Les États utilisent tous les outils à leur disposition pour défendre leurs intérêts. Jusqu'à présent, la réponse de l'Europe n'a pas réussi à éviter deux écueils : des efforts nationaux non coordonnés d'un côté ; une confiance aveugle dans la capacité des forces du marché à créer de nouveaux secteurs de l'autre.* »[13] Ainsi, face aux géants américain et

---

[7] The White House, *America First Investment Policy*, Memorandum, 21 février 2025.

[8] La République populaire de Chine, *La sécurité nationale de la Chine dans la nouvelle ère*, Bureau d'information du Conseil d'État, Agence de presse Xinhua, 12 mai 2025, http://www.mod.gov.cn/gfbw/fgwx/bps/16385614.html, consulté le 17 octobre 2025.

[9] Katja Drinhausen et Helena Legarda, « Comprehensive National Security" unleashed: How Xi's approach shapes China's policies at home and abroad », Mercator Institute for China Studies-MERICS, Rapport, 15 septembre 2022.

[10] *Ibid*.

[11] Haut Représentant de l'Union pour les Affaires étrangères et la Politique de sécurité, « COMMUNICATION CONJOINTE AU PARLEMENT EUROPÉEN ET AU CONSEIL RELATIVE À LA « STRATÉGIE EUROPÉENNE EN MATIÈRE DE SÉCURITÉ ÉCONOMIQUE » », 6 juin 2023.

[12] Commission européenne, « La Commission annonce miser sur la stratégie pour renforcer la sécurité économique de l'Europe », Communiqué de presse, 3 décembre 2025. Le programme ResourceEU, inclus dans les nouvelles mesures, vise à sécuriser l'accès aux matières premières critiques et aux semi-conducteurs.

[13] Mario Draghi, *High Level Conference – One year after the Draghi report: what has been achieved, what has changed*, discours devant la Commission européenne, Bruxelles, 16 septembre 2025, https://commission.europa.eu/topics/competitiveness/draghi-report/one-year-after_en?prefLang=fr&etrans=fr, consulté le 22 septembre 2025.

chinois désinhibés qui n'hésitent pas, pour atteindre leurs fins, à mobiliser sans retenue et dans tous les domaines un arsenal de moyens aussi agressifs que créatifs, et notamment leurs services de renseignement, mais aussi face à bien d'autres acteurs régionaux, l'Union européenne devrait selon lui s'affirmer davantage et, par le biais d'un « fédéralisme pragmatique », se placer à la bonne échelle pour mieux défendre et promouvoir ses intérêts[14].

À l'évidence, la mobilisation et la consolidation de chacun des pays membres conditionnent la réussite d'une telle entreprise et l'atteinte des objectifs associés par la production d'un effet de puissance collective adapté à l'ampleur du défi. Or, ces pays sont eux-mêmes plus ou moins déterminés ou aptes à défendre les intérêts d'une Europe-puissance conçue comme un acteur géopolitique souverain et autonome, les uns, au premier rang desquels la France, y œuvrant au nom du « salut collectif » et d'une vision éminemment politique de la puissance[15], les autres, l'Allemagne ou les Pays-Bas par exemple, semblant privilégier une approche économique exploitant les possibilités considérables du marché européen dans le « grand jeu » international[16]. Par ailleurs, les États membres sont eux-mêmes mutuellement en proie à une concurrence interne particulièrement agressive et hostile parfois, ce qui contraint dans certains cas les ambitions affichées et ouvre autant de failles à exploiter par la concurrence (voir Partie 2, 23).

Dans ce contexte, la France, en tant que deuxième économie de la zone euro et « puissance moyenne à vocation globale »[17], est donc elle aussi mise au défi. Les études, rapports, articles, discours, législations, mesures diverses ou encore initiatives publiques et privées en matière de sécurité économique abondent depuis quelques années, ce dont on ne peut que se féliciter[18]. La prise de conscience aurait eu lieu[19], les acteurs nationaux, dont les services de renseignement, sont effectivement mobilisés et d'incontestables progrès seraient réalisés[20]. Pourtant, tout en reconnaissant les efforts entrepris, la plupart des experts du domaine demeurent sceptiques voire inquiets, les uns les jugeant trop défensifs, timides ou dispersés, les autres allant jusqu'à considérer que la France dans son ensemble, contrairement aux assertions officielles, n'a pas pris la mesure du défi ni compris, ou voulu comprendre, la véritable teneur du « grand jeu » géo-économique en cours, y compris au sein de l'UE[21]. Peut-être touche-t-on là à une spécificité française : notre difficulté à participer à ce « grand jeu » et à mobiliser les acteurs en vertu d'un certain « patriotisme économique » nous incite à durcir à l'excès nos dispositifs de protection, avec pour conséquences une rigidification de notre écosystème et son corollaire, une invitation à leur contournement par les acteurs étrangers, dans une logique d'escalade potentiellement contreproductive.

Nous le verrons, cette critique est justifiée. Mais elle ne doit pas nous conduire à nous enliser dans des querelles de nature épistémologique. Ici, à l'instar de ce que font d'ailleurs nos principaux concurrents

---

[14] *Ibid*.

[15] Mathieu Duchâtel, « Comment penser la sécurité économique ? », Institut Montaigne, *Note d'enjeux*, mars 2024.

[16] Nicolas Ravailhe, entretien, 27 octobre 2025.

[17] Telle est la formule utilisée par Maurice Gourdault-Montagne à l'occasion d'un entretien au Point le 8 octobre 2022.

[18] On citera, parmi les derniers en date, le rapport Lienemann-Lemoyne de 2023, le rapport d'activité 2022-2023 de la Délégation Parlementaire au Renseignement-DPR, le rapport Plassard sur la « *guerre économique* » de 2025, le rapport Roux de Bézieux sur la sécurité économique de 2024 ou encore les travaux de l'EGE sur la contre-intelligence économique.

[19] Cette affirmation est généralement reprise par la plupart des rapports précités, avec toutefois des nuances.

[20] On fait ainsi référence, entre autres, au recours accru au dispositif de contrôle des investissements étrangers en France (CIEF) par la Direction générale du Trésor (DGT).

[21] C'est notamment la thèse de MM. Christian Harbulot (EGE), Alain Juillet, Nicolas Moinet et Nicolas Ravailhe.

et adversaires, nous promouvons une conception holistique de la sécurité économique, non pas réduite à un arsenal de mesures plus ou moins protectrices ou protectionnistes, mais appréhendée dans son grand objectif visant à protéger, consolider, développer et promouvoir un écosystème national, dans un contexte d'interdépendance globalisée, qui garantisse à la fois la souveraineté de la nation et son développement socio-économique selon les standards qu'elle se fixe à elle-même.

Quelle est donc la situation que connaît la France sur le plan de la sécurité économique ? De quelles capacités d'action dispose-t-elle face aux menaces et mesures hostiles, d'où qu'elles viennent, qui ciblent ses entreprises au quotidien ? Notre pays peut-il, doit-il, mieux faire ? De quelle manière ?

C'est en cherchant à répondre à ces questions que nous sommes arrivés à la conclusion que seules l'élaboration et la mise en œuvre à l'échelle nationale d'une stratégie de souveraineté et de sécurité économiques permettraient à la France de faire face efficacement à l'ingérence économique et de se positionner en acteur crédible et puissant, aux yeux de ses alliés et partenaires comme de ses adversaires, dans un environnement ultra-concurrentiel où règne la loi du plus fort. Comprendre son environnement et les mécanismes du « grand jeu » géo-économique qui s'y déroule, avoir une vision et fixer un cap, définir ses intérêts et appréhender de manière réaliste les menaces, se donner des objectifs en conséquence et saisir voire susciter les opportunités, telles sont les composantes majeures d'un nécessaire agir collectif, à la fois réactif et proactif. Cet agir doit en outre être opérationnalisé au travers d'une structure – nous proposons de mettre sur pied un état-major aux prérogatives décisionnelles placé sous l'autorité de la Présidence ou du Premier ministre. Seule cette approche permettra de définir et de conduire une véritable stratégie, à la convergence du politique et de l'opérationnel, débarrassée des oripeaux de l'idéologie et ancrée dans « le monde tel qu'il est ».

Ainsi, après avoir décrit le contexte international et rappelé ou proposé quelques éléments de définition, nous effectuerons dans un premier temps l'état des lieux dynamique de la menace à laquelle la France est confrontée (nature, acteurs – dont services de renseignement – objectifs et évolutions), au travers notamment d'études de cas concernant certains de nos alliés, partenaires et adversaires puis, dans un deuxième temps, nous nous livrerons à une analyse critique des dispositifs en place, publics et privés, destinés à protéger voire promouvoir les intérêts économiques nationaux[22]. Enfin, nous présenterons un certain nombre de recommandations, entendues comme autant d'axes d'effort ou lignes d'opérations, articulées autour d'une proposition centrale, l'établissement d'une stratégie nationale de souveraineté et de sécurité économiques.

[22] Présidence de la République, CNRLT, *Stratégie nationale du renseignement - SNR*, janvier 2025, file:///C:/Users/ddrgr/Downloads/snr_202501_fr%20(3).pdf, consulté le 8 septembre 2025.

Partie 1 - Les ingérences économiques en France : nature et ampleur du défi

11 - Éléments de cadrage et définitions

Le contexte international : l'entrée dans une nouvelle ère des relations internationales

Il nous semble impératif, avant d'analyser plus en détail le phénomène de l'ingérence économique, de prendre en compte avec la plus grande objectivité possible les évolutions contemporaines du contexte géopolitique. Voir le monde tel qu'il est, au travers de la dynamique des rapports de force entre puissances, constitue un prérequis indispensable à toute analyse réaliste et utile.

Dans son introduction à la Revue Nationale Stratégique (RNS) 2025, le président de la République affirme d'emblée : « Nous sommes à un point de bascule »[23]. Ce constat s'inscrit dans la continuité d'observations antérieures, exposées dès 2017 dans la Revue stratégique (RS) du MINARM[24], reprises et développées en 2020 dans le discours sur la stratégie de défense et de dissuasion prononcé à l'École de guerre[25], ou encore en 2021 (actualisation de la RS)[26] puis en novembre 2022 dans la première version de la RNS[27].

Le monde serait donc à un point de bascule. Pour beaucoup d'observateurs avertis, et cette nuance que nous partageons n'est pas anodine, le monde aurait en fait déjà basculé : l'ordre international libéral, dont l'avènement triomphal à l'occasion de l'effondrement de l'Empire soviétique promettait à l'humanité l'entrée dans une nouvelle ère, celle de « la fin de l'histoire »[28] et de l'avènement de la démocratie libérale, est aujourd'hui ébranlé et contesté. Dans les faits, la période d'hégémonie américaine aura duré environ trente ans avant de se déliter sous la pression d'un double phénomène d'émergence et d'affirmation de puissances soit « révisionnistes », soit tout simplement concurrentes.

Certes, la puissance américaine demeure inégalée et redoutable. Mais Washington, avec une lucidité et un pragmatisme qu'il convient de reconnaître, a fait ces dernières années le constat de l'érosion de sa puissance relative et en tire aujourd'hui des conclusions qui l'amènent à se raidir, jusqu'à saper les fondements même de l'ordre international bâti sous son égide. Parmi les principaux facteurs expliquant cette évolution, on retiendra :

L'affirmation chinoise, sous la forme du rival systémique et non d'un alter ego, fantasmé par l'hybris occidentale, appelé inéluctablement à se démocratiser. Le grand pari occidental de la mutation politique de la Chine sous l'influence du progrès économique aura été une illusion. On verra ainsi que dans ses ambitions sur le plan de la puissance et de l'économie, mais aussi par ses actions et ses méthodes, la Chine agit de plus en plus en miroir des Etats-Unis.

[23] SGDSN, *Revue nationale stratégique 2025*, Introduction, 13 juillet 2025.
[24] Ministère des Armées, *Revue stratégique de défense et de sécurité nationale*, octobre 2017.
[25] Élysée, *Discours du Président Macron sur la stratégie de défense et de dissuasion*, École de Guerre, 7 février 2020.
[26] Ministère des Armées, *Actualisation stratégique 2021*, DGRIS, janvier 2021.
[27] SGDSN, *Revue nationale stratégique-RNS*, 9 novembre 2022, https://www.sgdsn.gouv.fr/publications/revue-nationale-strategique-2022, consulté le 2 octobre 2025.
[28] Francis Fukuyama, *The End of History and The Last Man*, Free Press, 1992.

La résurgence russe, une puissance assertive certes bien moins performante que la Chine, mais à l'influence et aux capacités de nuisance redoublées.

Le phénomène plus global de l'émergence, qu'incarne par exemple l'accession de l'Inde au rang de puissance régionale à vocation globale, c'est-à-dire le développement économique et l'affirmation politique subséquente de puissances régionales déterminées à peser davantage sur les affaires du monde face à un Occident « dominateur » perçu comme de moins en moins légitime[29].

Les contrecoups de la mondialisation, pourtant portée par l'Occident mais dont certains effets, notamment sur le plan économique - la désindustrialisation en particulier (les Etats-Unis, le Royaume-Uni et la France, contrairement à l'Allemagne, en sont des exemples emblématiques) - ont contribué à abîmer les modèles socio-économiques des nations concernées et à saper la confiance dans les gouvernements successifs.

Ainsi, la phase de transition que nous vivons voit se mettre en place de nouveaux équilibres, ou déséquilibres, par le recours à un arsenal de moyens et de méthodes de plus en plus désinhibés, incluant la force militaire. Dans tous les domaines et milieux, l'intimidation, la coercition, la prédation et la combinaison de multiples instruments d'affirmation de puissance souvent dévoyés de leur but premier – que l'on tend à ranger sous le vocable de « menaces hybrides » - sont déployés avec agressivité au quotidien.

Les leviers économiques sont utilisés à des fins politiques, le renseignement à des fins économiques. Les entreprises sont plus que jamais des cibles mais aussi des capteurs, via notamment le jeu des multiples affiliations nationales au sein des grands groupes en particulier. Au cœur du modèle se trouvent les données, soit de masse, au service de l'IA, soit spécifiques aux entreprises. Dans ce contexte où, comme le souligne le rapport Roux de Bézieux, la géopolitique est entrée dans les conseils d'administration et où la numérisation contribue à fragiliser les écosystèmes, le rôle des services de renseignement dans la recherche et la collecte de l'information est déterminant.

L'arme économique et le « nationalisme économique décomplexé »[30]

Ainsi l'économie, comme le droit d'ailleurs, est aujourd'hui, plus encore qu'hier, une arme au service de politiques de puissance nationales de plus en plus agressives dans le cadre d'une compétition internationale impitoyable. Guerre économique ou pas, l'« arsenalisation » (« *weaponization* ») des instruments de puissance est une réalité, tantôt pleinement assumée, tantôt décriée[31]. Les principales puissances, États-Unis et Chine en tête, font dès lors de la sécurité économique un élément central de la sécurité nationale conçue sur des plans aussi bien offensifs que défensifs[32]. La convergence actuelle aux Etats-Unis des intérêts de la *New Tech* et des GAFAM qui « veulent des rentes, pas la compétition » (« *want rents, not competition* ») et du gouvernement Trump qui « veut le pouvoir » (« *wants power* ») en est symptomatique[33].

---

[29] Nous renvoyons ici au discours de M. Vladimir Poutine prononcé à l'occasion de la Conférence de sécurité de Munich, édition 2007, ou encore, plus récemment, à la « doctrine Karaganov » dite de la « majorité mondiale » dont une traduction est proposée par *Le Grand Continent*, « *Désoccidentaliser le monde : la doctrine Karaganov* », 20 avril 2024.

[30] Martin Videlaine et Guillaume Caudron, *Réindustrialiser*, Paris, Dunod, 2024, p. 17.

[31] Henry Farrell et Abraham Newman, *L'empire souterrain*, Paris, Odile Jacob, 2024.

[32] Cas emblématique de Nexperia qui démontre, si besoin en était, combien la rivalité géopolitique sino-américaine agit sur les rapports de force économiques et touche directement aux intérêts des différents acteurs des chaînes de valeur, par intimidation ou coercition.

[33] Henry Farrell et Abraham Newman, *op. cit*. La *New Tech* fait référence aux entreprises de l'écosystème des nouvelles technologies ; les GAFAM sont : Google, Amazon, Facebook, Apple et Microsoft.

Afin de mieux cerner les contours de la « sécurité économique », interrogeons-nous dans un premier temps sur le concept de « sécurité nationale », un concept mal défini, sujet à de nombreuses interprétations, qui pourtant est invoqué régulièrement par certains de nos partenaires pour justifier de mesures parfois hostiles à l'encontre de leurs concurrents.

Du concept de « sécurité nationale »

Donner une définition générique de la sécurité nationale est une gageure dans la mesure où elle est par essence subjective puisque dépendante des critères de jugement et d'évaluation fixés par le pays concerné en fonction de sa propre perception de la menace et de ses intérêts. Pour autant, on peut avancer qu'elle comprend une logique première de souveraineté : il s'agit originellement de se protéger contre toute menace directe ou indirecte pouvant porter atteinte à l'intégrité du territoire et de sa population (mission première), ainsi qu'au développement de la société concernée. Ce second point est essentiel, car il traduit l'idée de volonté nationale et de représentation de soi, mais aussi de projection éventuelle de ses aspirations et idéaux. Il implique donc de disposer des moyens et instruments nécessaires à une prise de décision autonome non soumise à de quelconques ingérences, à l'affirmation de son modèle national et, par voie de conséquence, au déploiement de différentes mesures et méthodes de toute nature qui permettent à la nation concernée de « tracer son chemin ». En second lieu, elle repose sur une logique pratique d'application plastique : le concept est par construction élastique et évolutif puisqu'il est censé non seulement permettre de répondre aux « menaces » de l'environnement extérieur, mais plus encore d'en créer soi-même pour autrui au besoin, d'anticiper afin de neutraliser par avance les possibles menaces, et de façonner indirectement par une attitude proactive les conditions de la relation stratégique en cause, en s'inscrivant dans une approche géopolitique d'exercice de la puissance.

Dès lors, restreindre ce concept à une dimension définitionnelle et pratique défensive serait une erreur de jugement : dans l'esprit et dans les actes des principales puissances, la dimension offensive, ou plutôt proactive, qu'elle soit de nature préventive, préemptive ou de conquête, est une priorité. Les Etats-Unis comme la Chine ont en effet une compréhension, et une pratique, extrêmement expansives et offensives de ce concept.

L'exemple américain est le plus parlant. Washington, dès la fin de la Seconde Guerre mondiale, a établi, via le *National Security Act*[34], un référentiel politico-stratégique[35] global et, surtout, cohérent. Depuis, stratégie économique et sécurité nationale sont indissociables, la stratégie macro-économique des Etats-Unis s'inscrivant dans la vision géopolitique de leur puissance. La *National Security Strategy* de novembre 2025 publiée par l'administration Trump II le rappelle en ces termes : « la sécurité économique est fondamentale pour la sécurité nationale »[36]. Le document fixe en la matière les grands objectifs suivants : l'équilibre commercial, la sécurisation de l'accès aux chaînes d'approvisionnement et aux matériaux essentiels, la réindustrialisation, la relance de la base industrielle de défense, la domination énergétique et, enfin, la préservation et le renforcement de la domination du secteur financier américain[37]. Comme le rappelait récemment l'Ambassadeur Vimont, trois piliers constituent cette vision géopolitique : la protection de la sécurité nationale, la puissance économique

[34] 1947 National Security Act, https://www.dni.gov/index.php/ic-legal-reference-book/national-security-act-of-1947, consulté le 3 octobre 2025.
[35] Philippe Hayez, Séminaire « Les entreprises françaises face aux services de renseignement étrangers », Paris, 28 janvier 2025.
[36] White House, *U.S. National Security Strategy*, novembre 2025, p. 14.
[37] *Ibid*., p. 13 et 14.

et financière, et l'organisation de l'État[38]. Historiquement, une phase d'accélération et de durcissement eut lieu après les attentats du 11-Septembre, à une époque où l'Amérique meurtrie, engagée dans la *Global War On Terror* (GWOT), avait décidé d'arsenaliser un certain nombre de fonctions stratégiques et de dispositifs régaliens (*lawfare* par exemple). Ensuite, l'émergence de nouvelles menaces dans un contexte d'érosion de la puissance relative de l'Amérique face à la Chine a encouragé les efforts d'adaptation de l'appareil américain et le durcissement d'un certain nombre de dispositifs, au point où tout ou presque ressortit désormais à la sécurité nationale : les services de l'État sont alignés et coopèrent étroitement, y compris le judiciaire, des lois aussi protectrices qu'offensives sont régulièrement votées (CHIPS *Act* de 2022[39] ; *Inflation Reduction Act* de 2023), et des mesures agressives déployées, telles que la politique des droits de douane en 2025. Plus encore, les États-Unis ont compris depuis longtemps le rôle déterminant du droit et de la norme. Dès les années 90, ils œuvrent à façonner l'écosystème international, surtout dans les domaines émergents, afin d'imposer leur vision de la norme et de pouvoir en tirer les bénéfices afférents (*U.S. Cloud Act* de 2018 par exemple[40]). Dans cet écosystème, la place des services de renseignement est essentielle pour collecter l'information indispensable à l'anticipation et à la compréhension des adversaires et concurrents, mais aussi pour identifier les vulnérabilités à exploiter, et pour influencer, intimider, contraindre, ou encore entraver d'éventuelles initiatives contraires aux intérêts américains.

La communauté du renseignement est donc parfaitement intégrée à l'écosystème stratégique national et met en œuvre ses instruments au service d'une vision globale et géopolitique dont le premier objectif consiste à prévenir l'ascension d'un hégémon régional[41]. Il y a aux Etats-Unis une synergie totale, naturelle et entretenue entre politique et renseignement, ce dont l'auteur de ce rapport peut attester. Le renseignement, acmé du politique, est l'arme stratégique par excellence[42]. Pour Washington, disposer d'une politique publique de renseignement est une évidence depuis la fin de la Seconde Guerre mondiale, laquelle se fonde d'ailleurs sur une longue tradition et une profonde sensibilisation aux menaces et risques. En atteste la mise en place dès 1938 du *Foreign Agents Registration Act* (FARA)[43], un instrument très complet et intrusif, depuis complété par le *Federal Election Campaign Act* (FECA)[44] de 1971 et le *Lobbying Disclosure Act* (LDA)[45] de 1995, qui permet aux autorités américaines d'exercer une vigilance et un contrôle sur les actions et éventuelles ingérences étrangères dans des domaines sensibles. Autre loi fondatrice, le *Foreign Intelligence Surveillance Act* (FISA), promulgué en 1978 et amendé à de multiples reprises depuis le 11-Septembre, est autant un instrument d'espionnage que d'exercice d'extraterritorialité du droit[46].

Ainsi, les débats qui ont secoué l'écosystème politico-administratif français lors des travaux sur l'établissement d'une politique publique de renseignement – et qui continuent d'animer certains

[38] Intervention de Monsieur l'Ambassadeur Pierre Vimont, « Les entreprises françaises face aux services de renseignement américains », op.cit.
[39] Il s'agit du « *Creating Helpful Incentives to Produce Semiconductors* (CHIPS) *Act* » du 9 août 2022, U.S. Congress.
[40] Il s'agit de la loi dite « *Clarifying Lawful Overseas Use of Data Act* (*Cloud Act*) » du 23 mars 2018, U.S. Congress.
[41] Allemagne et Japon durant la Deuxième Guerre mondiale, Russie soviétique pendant la Guerre froide, Chine aujourd'hui.
[42] Georges-Henri Soutou, « La stratégie du renseignement : essai de typologie », *Stratégique*, 2014/1 N° 105, pages 23 à 42, Éditions Institut de Stratégie Comparée.
[43] Department of Justice (DoJ), https://www.justice.gov/nsd-fara, consulté le 10 octobre 2025.
[44] U.S. Congress, https://www.govinfo.gov/content/pkg/COMPS-985/pdf/COMPS-985.pdf, consulté le 10 octobre 2025.
[45] U.S. Congress, https://www.congress.gov/bill/104th-congress/senate-bill/1060, consulté le 10 octobre 2025.
[46] Andreas Kuersten, « *Foreign Intelligence Surveillance Act* », IF11451, CRS, 17 décembre 2024, https://www.congress.gov/crs-product/IF11451, consulté le 10 octobre 2025.

cercles universitaires – sont difficilement compréhensibles aux Etats-Unis. Comment peut-on revendiquer une certaine puissance et une influence sur les affaires du monde, et reléguer la fonction renseignement au rang de simple instrument parmi d'autres, voire la rejeter à l'extérieur du périmètre légitime de l'action publique ? Pour un esprit américain, anglo-saxon en général, et cela est valable chez bien d'autres[47], le renseignement est un outil de nature éminemment politique qui est au cœur de toute stratégie d'influence.

La communauté du renseignement américaine (*Intelligence Community*-IC)[48] se compose de 18 agences disposant d'un budget d'environ $100 MdS en 2025[49]. Elle est au service d'une puissance globale qui a développé une culture stratégique et de renseignement selon les lignes de force suivantes :

Le contrôle à distance, favorisé par une forme d'insularité et manifesté par le réseau des *Five-Eyes.*

L'influence assumée, légitime et positive, qui consiste, par l'acquisition de l'information et du savoir, à façonner l'environnement et les acteurs internationaux.

L'intégration dans la société (discours) et l'écosystème académique (Intelligence Studies) qui confère au renseignement toute sa légitimité voire sa « noblesse ».

Le partenariat public-privé, de plus en plus resserré, notamment dans le domaine économique, scientifique et technologique (voir le rapprochement accéléré entre le Pentagone et la Silicon Valley par exemple).

Enfin, puissance globale oblige, la culture du renseignement est marquée par la recherche quasi obsessionnelle de l'omniscience[50], et favorise pour cela une approche scientifique et techniciste portée par la maîtrise des nouvelles technologies.

De la sécurité économique

L'économie est donc à la fois un facteur majeur de puissance et un domaine d'exercice de celle-ci. Là encore, la notion de sécurité économique, dans son acception première et originelle, fait référence, selon une logique bienveillante de « bonne gouvernance »[51], à la protection de l'individu et du système socio-économique, comme la sécurité nationale fait référence à la protection du territoire national et de la population. Bien évidemment, dans le contexte précédemment décrit qui est le nôtre, le concept s'élargit et se manifeste désormais par ce que des chercheurs américains appellent la « *weaponization of economic interdependence* », non plus selon une logique de « *mutual dependence* » mais de « *asymetrical dependence* »[52].

À l'échelle des rapports de force mondiaux, deux approches types de la sécurité économique coexistent. M. Duchâtel note en effet que l'UE tend à privilégier une approche strictement économique dans son appréhension des enjeux, fondée sur la gestion du risque, alors que d'autres puissances, au premier rang desquelles les États-Unis, la Chine ou le Japon par exemple, ont toujours privilégié une lecture géopolitique par construction plus globale, plus cohérente et plus offensive ou

[47] La Chine et la Russie sont des exemples emblématiques dans ce domaine.
[48] Voir Annexe 2 – *La Communauté américaine du renseignement*.
[49] National Intelligence : $73,4 MdS. La demande pour 2026 s'établit à $81,9 MdS. Military Intelligence : $28,2 MdS.
[50] Selon Roger George, ancien professeur du U.S. National War College : « Tout savoir sur tout ; tout concerne l'Amérique ». Propos tenus le 22 septembre 2023 à l'occasion d'un échange par visioconférence au profit des étudiants du Mastère renseignement de l'IEP d'Aix-en-Provence.
[51] Mathieu Duchâtel, Institut Montaigne, op.cit.
[52] Henry Farrell et Abraham Newman, « *Foreign Affairs Interview* », 2025.

proactive[53]. Cela étant, quel que soit le modèle, la sécurité économique implique un certain degré d'interventionnisme étatique, ce qui vient heurter les grands principes du libéralisme économique d'une part, et fait d'autre part de l'économie un instrument de plus en plus mobilisé au service d'impératifs de sécurité nationale expansifs. Les caractéristiques de l'environnement stratégique actuel marqué par l'agressivité contraignent chaque jour davantage les différents acteurs à prendre des mesures dites de « sécurité économique », ne serait-ce que pour limiter l'impact des agressions répétitives. Or, il s'agit là d'une lecture restrictive du concept : hors UE, élaborer et conduire une politique industrielle est une priorité, mobiliser tous les instruments au service d'une vision géopolitique une évidence[54], et promouvoir des politiques normatives ou d'extraterritorialité du droit une démarche assumée[55].

On relèvera d'emblée qu'en ce domaine, la position française est originale et paradoxale. En Europe, comme nous le verrons plus en détail (voir Partie 2, 22), la France est sans doute le pays traditionnellement le mieux armé sur le plan de la sécurité économique, entendue dans son acception restrictive de dispositif de protection, grâce à un ensemble de dispositions juridiques et réglementaires qui orientent de nombreux organismes chargés d'exercer une vigilance et de prendre les mesures adéquates pour protéger les intérêts et actifs stratégiques français. Or, et là s'affirme le paradoxe, les dernières décennies ont vu les capacités industrielles de la France s'affaiblir[56], son avantage comparatif s'éroder dans bien des domaines stratégiques[57], et ses partenaires et concurrents se livrer à des actions d'ingérence, parfois particulièrement agressives, sans retenue (la présence chinoise par le contrôle d'entreprises s'est densifiée en France plus encore que chez nos principaux concurrents européens)[58].

De l'intelligence économique et de l'influence

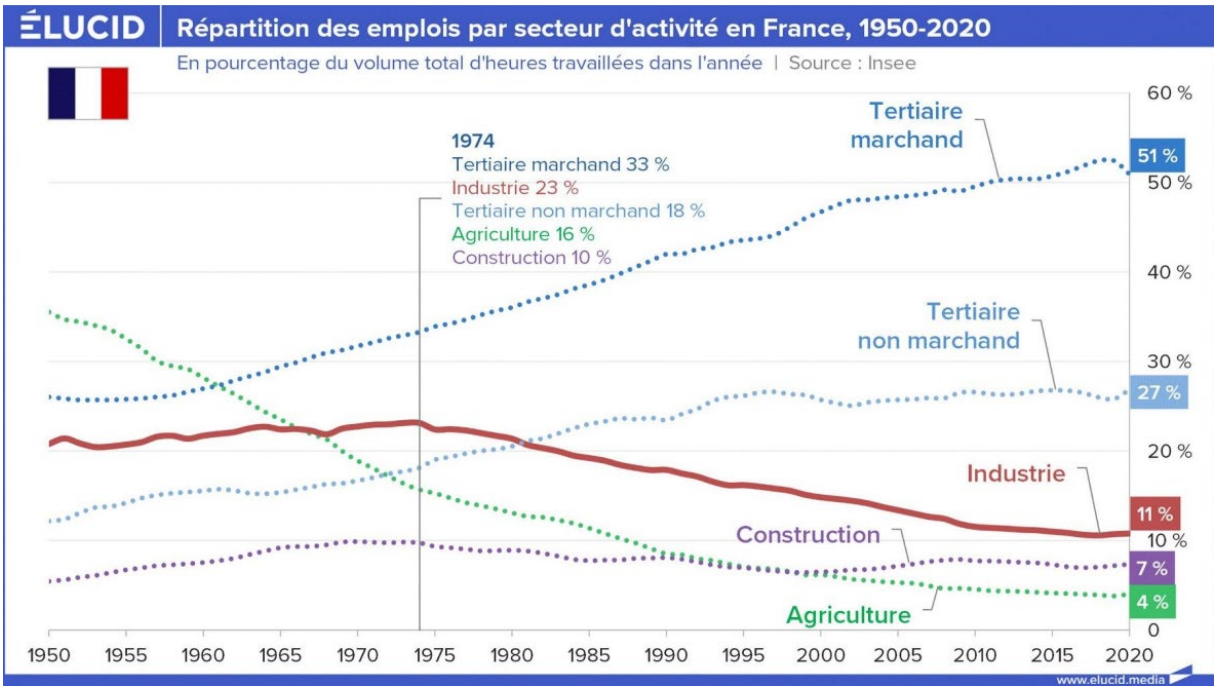
« Alternativement présentée comme une dynamique, une culture, une méthode, un mode de gouvernance, un mode de pensée et d'action, une démarche ou encore un domaine de recherche, l'intelligence économique vise avant tout à **se « mettre en alerte »** afin de **défendre les intérêts stratégiques** d'un État, d'une entreprise, d'un territoire ou d'un établissement de recherche et d'en **promouvoir la compétitivité**. Cela repose sur les **trois séries d'actions** suivantes : la veille stratégique ou concurrentielle ; la protection du patrimoine matériel ou immatériel ; les opérations d'influence »[59].

C'est ainsi que le rapport Lienemann-Lemoyne présente l'intelligence économique. Il faut donc comprendre « intelligence » en son sens premier de capacité à appréhender son environnement dans toutes ses dimensions et ramifications, et à l'influencer. En ce sens, l'information (dont les données) est au cœur de la compétition économique : la rechercher, la capter, l'exploiter, la manipuler, etc. sont aujourd'hui des missions essentielles qui conditionnent en grande partie la valeur, le potentiel et l'effectivité de toute stratégie ou démarche d'affirmation économique.

[53] Mathieu Duchâtel, Institut Montaigne, *op.cit.*
[54] Mathieu Duchâtel, Institut Montaigne, *op.cit*., à propos de la vision américaine de l'*IndoPacific Economic* Forum (IPEF).
[55] *Ibid.*
[56] Voir schéma infra, p. 18.
[57] On citera, entre autres : Alcatel, les pertes subies par Alstom, Areva, etc.
[58] Nicolas Ravailhe, entretien, *op.cit*.
[59] Rapport Lienemann-Lemoyne, *op.cit.*

État des lieux sommaire des forces et faiblesses de l'économie française

Comme le mentionne le rapport Lienemann-Lemoyne de 2023, depuis les années 80, la France connaît « une perte de souveraineté profonde et transversale » qui se traduit par le phénomène de désindustrialisation et la perte continue de parts de marchés[60]. Alors que le gouvernement promeut une politique de réindustrialisation et que plusieurs initiatives ou programmes sont mis en œuvre, dont le Plan Relance 2030, il convient de s'interroger sur les progrès réalisés et les difficultés rencontrées.



Source : IGPDE, Infographie La Désindustrialisation de la France: 1995-2015

À partir des statistiques officielles[61], nous constatons que la France a subi la concurrence internationale dans un certain nombre de secteurs ou filières stratégiques au fil des ans, entraînant la perte de fleurons industriels ou l'érosion de son avance technologique dans d'autres. Ainsi, « entre 1995 et 2024, la part de l'industrie dans le PIB national s'est effondrée de 17 % à 10 % […]. En 30 ans, nous avons perdu près de deux millions d'emplois industriels »[62].

Aujourd'hui, à l'heure de la réindustrialisation, le constat est mitigé[63]. Dans ce domaine, l'EGE vient de publier un état des lieux établi à partir d'un outil de diagnostic destiné à mesurer les risques de désindustrialisation qui repose sur plusieurs critères tels que le positionnement stratégique (état des dépendances), la situation financière, la vulnérabilité technologique, la gouvernance ou encore les

[60] *Ibid.*
[61] IGPDE, *La Désindustrialisation de la France : 1995-2015*, Infographie, https://www.economie.gouv.fr/files/files/directions_services/igpde-seminaires-conferences/Infographie%20D%C3%A9sindustrialisation%20-%20Dufourcq.pdf, consulté le 3 novembre 2025.
[62] Arnaud de Morgny, EGE, cité dans : Florent Godard, « ArcelorMittal, Renault, Valeo… : Un nouvel indicateur mesure le risque de désindustrialisation en France », *Le Journal des Entreprises*, 29 septembre 2025.
[63] Pierrick Merlet, « La France poursuit sa lente désindustrialisation », *La Tribune*, 29 juillet 2025, https://www.latribune.fr/entreprises-finance/industrie/la-france-poursuit-sa-lente-desindustrialisation-1030503.html, consulté le 5 novembre 2025.

risques géopolitiques[64]. Du bilan provisoire actuel, il ressort que trois entreprises sont en situation de grande vulnérabilité (risque de 3,5 sur 5) : ArcelorMittal, Renault et Valeo. Arkema (3), Michelin (2,8) et le Groupe Seb (2,7) sont en situation de vigilance.

Au-delà de la situation hexagonale, soulignons le risque de dépendance technologique accrue pour l'Union européenne dans la mesure où, selon certains experts, sur les 47 technologies d'avenir répertoriées, 37 seraient maîtrisées par la Chine, 8 par les Etats-Unis et seulement 3 par l'UE.[65] Cette dernière est d'ailleurs consciente des risques encourus et se mobilise pour y faire face[66].

Dans un deuxième temps, abordons la question de la définition de la menace et de sa compréhension par la France.

12 - État des lieux de la menace

À partir des nombreuses dispositions règlementaires prises ces dernières années, des conférences et autres séminaires régulièrement tenus par différentes institutions, et des entretiens effectués avec les principaux acteurs publics et privés du domaine, y compris du monde du renseignement, nous tenterons d'exposer une typologie de la menace en prenant soin de la replacer dans le contexte de l'évolution des rapports de force présentée supra.

Tentative de définition de la « menace »

Comment comprendre la notion de menace ?

La charge cognitive du terme étant négative, elle peut aisément contribuer à instiller dans les esprits une sensibilité de citadelle vertueuse assiégée, convoitée par des puissances extérieures qui, par des actions hostiles, illégitimes voire illégales, viendraient injustement corrompre un environnement national – ou européen – respectueux de règles universelles, en vigueur depuis la fin de la Seconde Guerre mondiale dans le cadre de la mondialisation dite libérale. Or, il y a là risque de confusion entre ce que certains estiment être la nature même de la compétition entre nations (*business is business*), donc parfaitement légitime, et ce que d'autres perçoivent comme excessif, déloyal ou inacceptable ; en un mot, entre influence et ingérence. La porosité entre les deux est manifeste et de plus en plus marquée voire manipulée[67]. Les uns n'hésitent pas à prendre des mesures de protection extrêmement rigoureuses face à ce qu'ils dénoncent comme autant de véhicules d'ingérences étrangères tout en enfourchant ce même destrier à l'assaut de leurs concurrents économiques ; les autres cherchent à dissiper le brouillard de la confusion et à discriminer les situations relevant de l'influence ou de l'ingérence, déplorant la transformation de la compétition naturelle censée être encadrée par des règles en « jeu pernicieux » fondé sur des « règles d'engagement » parfois illégales. En conséquence, les tenants de la deuxième proposition pourront avoir tendance à ériger en absolu leur système de référence pourtant de facto contesté, et dès lors à réduire l'éventail de leurs possibilités d'action au nom de principes supérieurs. Ils tendront ainsi à privilégier deux approches : la première consistera à s'en tenir malgré tout au respect des règles censées régir le modèle économique international et ainsi à accorder une confiance quasi naïve au jeu du marché, ce que dénonce M. Draghi par exemple[68], tandis que la seconde les incitera à s'interdire des actions non conformes à leurs principes, pourtant

[64] CR 451, [Rapport] *Anticiper la désindustrialisation : un indice pour anticiper la désindustrialisation et réarmer l'intelligence économique territoriale*, EGE, 16 juillet 2025, https://cr451.fr/wp-content/uploads/2025/07/EGE-CR451_IndiceDe%C2%B4sindustrialisation_VF2-compresse.pdf, consulté le 3 décembre 2025.
[65] Alain Juillet, *Les freins à la réindustrialisation*, Sénat, audition du 27 mars 2024.
[66] Voir l'actualisation de la stratégie de sécurité économique de l'UE et le programme *ResourceEU*, op.cit.
[67] DPR, rapport d'activité 2022-2023, *op.cit.*
[68] Discours du 16 septembre 2025, Bruxelles, *op.cit.*

nécessaires pour tenter, autant que faire se peut, de maintenir leurs propres capacités et leur potentiel en situation de crédibilité suffisante pour imposer en retour leurs vues.

Qu'est-ce qu'une ingérence économique ?

Dans son rapport d'activité pour l'année 2022-2023, la DPR donne la définition suivante de l'ingérence : « l'ingérence renvoie à une action dissimulée et malveillante. Commanditée depuis l'étranger, elle vise à porter atteinte, autrement que par la confrontation militaire, aux intérêts fondamentaux d'un pays et à sa souveraineté dans toutes ses dimensions politique, juridique, militaire, économique et technologique ». La DPR et les services identifient historiquement trois formes d'ingérence : classique (espionnage, débauchage, etc.), moderne (domaines cyber, spatial, etc.) et hybride (influence, manipulation de l'information, diversité des acteurs). Ils soulignent qu'aujourd'hui, ces formes se combinent dans le but de perfectionner les actions d'interférence et de corrompre les processus décisionnels des systèmes visés.

Sur le plan économique, il s'agit donc de toute action ou mesure, conduite ou commanditée par un État ou un organisme étranger, de nature hostile et intrusive, et donc subie, qui s'attaque aux intérêts et à la souveraineté économiques de la nation concernée. Ainsi, pour la DRSD, en charge de la protection de la base industrielle et technologique de la défense (BITD), une ingérence est « un acte hostile visant à porter atteinte, autrement que par la confrontation militaire directe, aux intérêts fondamentaux de la Nation ainsi qu'à la défense nationale et au secret de la défense »[69].

Toutes les études convergent aujourd'hui pour le souligner et le rappeler : la France fait face à une menace « devenue protéiforme, omniprésente et qui s'inscrit dans la durée »[70].

Dans les faits, la situation est d'autant plus délicate que la porosité entre influence et ingérence est de plus en plus développée et assumée. Là encore, à chaque fois, l'ingérence sera identifiée, évaluée et éventuellement contrebattue à l'aune de nos propres impératifs, contraintes et besoins. Pour distinguer l'influence de l'ingérence, on se repose sur les critères d'agressivité et d'illégalité[71]. En tant que telle, l'agressivité n'est pas illégale et ne justifie pas forcément pour un acte la qualification d'ingérence, celle-ci étant, au regard du droit, caractérisée par l'illégalité. En conséquence, la notion d'ingérence est particulièrement complexe à appréhender, ce que traduit la directrice de la DGSI, Mme Berthon, dans son entretien aux Échos par : « pernicieuse »[72]. En effet, une action adverse de prise de participation dans une société considérée comme un « acteur stratégique » pourra être perçue et combattue comme une ingérence par tel pays, ou être tolérée par tel autre en raison d'une dépendance financière qui le portera à privilégier une forme de coopération et à accepter un certain niveau de risque plutôt qu'à encourir une éventuelle perte sèche, au nom d'un impératif d'attractivité de son économie. On parle alors de « zone grise », comme on le fait dans le domaine des menaces hybrides d'ailleurs.

On retiendra donc que la notion de menace recèle deux volets : la dimension offensive ou agressive de type OPA hostile, laquelle n'est pas forcément illégale, et la vulnérabilité, typiquement issue d'une situation financière délicate, qui présente une opportunité pour le concurrent[73]. Sur ce point, les

[69] DRSD, https://www.defense.gouv.fr/drsd/contre-ingerence-economique, consulté le 8 septembre 2025.
[70] DPR, *op. cit*.
[71] DGSI, Entretien, 7 novembre 2025.
[72] Céline Berthon, *Les Échos, op.cit.*
[73] DGSI, Entretien, 7 novembre 2025.

données fournies par la DGSI sont très éclairantes : sur 2000 alertes annuelles environ, 10% sont des ingérences tandis que 90% correspondent en réalité à des situations de vulnérabilité[74].

Les acteurs : compétiteurs, « partenaires-concurrents » ou adversaires

Un constat préoccupant

En matière d'ingérence à l'encontre des entreprises françaises en général (environ 240 000 entreprises dont 8000 dans des filières dites stratégiques)[75], et de la BITD en particulier (9 grands groupes et 4500 ETI-PME-Startups soit 220000 emplois)[76], Etats-Unis et Chine représentent à eux deux les deux tiers des actions hostiles tous domaines confondus[77]. Suivent les partenaires européens, principalement l'Allemagne et l'Italie, puis les partenaires du PMO, Israël et les pétromonarchies. La Russie est présente, certes, mais la menace qu'elle constitue dans ce domaine est très ciblée, procède d'une logique de nuisance, et est moins inquiétante sur le strict plan économique que celle des partenaires européens cités.

Selon le Service de l'Information Stratégique et de la Sécurité Économiques (SISSE), on recense environ 1000 alertes par an depuis quelques années, dont 50% sont de nature capitalistique[78]. Une proportion non officiellement communiquée, mais reconnue comme très significative de ces alertes capitalistiques sont le fait des seuls États-Unis. La DRSD quant à elle recense environ 600 actes d'ingérence par an dont près de la moitié sont d'origine humaine[79]. Les Etats-Unis sont le premier « ingérent défense » en France, suivis par la Chine puis, à moindre niveau, la Russie, la Turquie ou encore Israël. L'analyse de la DRSD pointe, à titre illustratif, les actions suivantes qui touchent principalement les nouvelles technologies de l'information et des communications (TIC), l'aéronautique et l'espace[80] :

- Humaines (débauchage de chercheurs, pressions exercées à l'occasion d'un déplacement à l'étranger) ;
- Physiques (intrusion au sein d'un laboratoire, survol de drone à des fins de reconnaissance) ;
- Capitalistiques (approche d'incubateurs de start-ups par des fonds étrangers activistes) ;
- Juridiques (inclusions de clauses à portée extraterritoriale dans un partenariat universitaire) ;
- Réputationnelles (campagne internationale de dénigrement des recherches développées par un laboratoire) ;
- Cyber (rançonnage d'un laboratoire ou exfiltration de données à des fins d'espionnage).

À partir des constatations faites par l'ensemble des acteurs français, et notamment des services, on peut dresser le tableau suivant de la situation :

- Menace capitalistique (prises de participation ou offres d'achat de nature hostile) : elle demeure la principale menace ;

[74] DGSI, « Les entreprises françaises face aux services de renseignement étrangers », intervention, Paris, 28 janvier 2025.

[75] Stéphanie Tison, sherpa de la Commission souveraineté et sécurité économiques, MEDEF, entretien du 21 octobre 2025.

[76] Direction générale de l'armement-DGA, https://www.defense.gouv.fr/dga, consulté le 22 septembre 2025.

[77] Ce constat est partagé par la CNRLT, le SGDSN, la DRSD et le SISSE.

[78] Mathieu Kahn, « *Les entreprises françaises face aux services de renseignement étrangers* », *op. cit.*

[79] DRSD, « *Les entreprises françaises face aux services de renseignement américains* », *op. cit.*

[80] *Ibid*. Ces éléments sont repris dans : Institut des Hautes Études de l'Éducation et de la Formation, *DRSD : un service de renseignement qui protège la recherche en lien avec la Défense – Entretien*, octobre 2024.

- Menace physique : elle demeure très prégnante et se décline sous de nombreuses formes. Citons les contrôles abusifs dans les aéroports, les visites indues dans des entreprises par des délégations mal contrôlées, les effractions, etc. ;
- Menace humaine : il s'agit principalement des actions de débauchage ;
- Menace réputationnelle ;
- Menace cyber : une catégorie en soi, toujours très active, permanente, un « défi sans fin »[81] ;
- Menace du *lawfare* : les actions en matière de normalisation et d'extraterritorialité constituent désormais un axe d'effort chez la plupart des compétiteurs, et notamment les Etats-Unis et la Chine.

Une juste appréhension de la menace repose sur la juste appréciation de l'évolution du contexte international et des rapports de force. En ce sens, la situation est préoccupante. En effet, les deux principaux acteurs engagés dans un affrontement systémique font preuve d'une agressivité – et d'une créativité - potentiellement destructrices pour bon nombre de concurrents[82]. Dans le cas des États-Unis, on assiste à la combinaison d'une politique visant à imposer un nouveau cadre de référence au commerce international via les droits de douane d'une part, et à une politique coercitive qui se manifeste par exemple en Europe sous la forme d'un chantage à la sécurité d'autre part. Du côté chinois, on assiste à un durcissement des positions dans les secteurs sensibles, mais aussi à un phénomène général de concurrence par la mise en œuvre de méthodes commerciales abusives qui peuvent déstructurer les tissus industriels des pays visés, en tous domaines[83].

À cela s'ajoute, dans un contexte de développement accéléré des technologies dites duales, donc d'une confusion grandissante entre les dimensions militaires et civiles[84], une radicalisation des postures qui se traduit par le déploiement de mesures de nature hybride pouvant aller jusqu'au positionnement d'actifs à des fins hostiles (neutralisation à distance d'infrastructures portuaires ou aéroportuaires pouvant paralyser l'économie d'un pays)[85], mais aussi par le renforcement des contrôles des produits échangés selon des règles de plus en plus complexes, et notamment le « *Reverse CFIUS* », dans le contexte d'un nationalisme économique assumé et de la tentative de la Chine d'asphyxier certains concurrents.

Dès lors, une lecture strictement économique de la situation qui se déploie sous nos yeux en méconnaîtrait la nature profonde qui relève, à l'évidence, de la rivalité de puissance à visée géopolitique. À ce stade, il est utile de se pencher sur le cas des deux « géants » en la matière.

Les Etats-Unis d'Amérique : une puissance à l'offensive

Les faits sont là : depuis des décennies, les Etats-Unis représentent la principale menace pour la France et, de manière générale, ses concurrents européens, dans le domaine économique. M. Pierucci le démontre, statistiques à l'appui : 60% des sociétés étrangères visées depuis les années 2000, souvent avec comme point de départ la mécanique de lutte contre la corruption qui repose sur le FCPA[86], sont européennes et sont des acteurs majeurs dans les secteurs de l'énergie (pétrole, nucléaire), de

[81] Information non attribuable.

[82] IGA (er) Jacques Roujansky, Chef de la majeure « Défense et sécurité économique », IHEDN, entretien du 7 octobre 2025.

[83] Voir le cas de l'entreprise Shein, par exemple.

[84] Mathieu Duchâtel, Institut Montaigne, *op. cit.*

[85] Jacques Roujansky, IHEDN, *op. cit*.

[86] https://www.justice.gov/criminal/criminal-fraud/foreign-corrupt-practices-act, consulté le 22 octobre 2025. On notera que l'administration Trump a mis en pause, par décret du 10 février 2025, les dispositions du FCPA à l'encontre des entreprises américaines, dans le but affiché, sans vergogne, de lutter contre une concurrence étrangère jugée déloyale.

l'aéronautique, du spatial et de la banque et, désormais, des nouvelles technologies[87]. On pourra dès lors s'étonner que Mme Berthon affirme : « Les Etats-Unis non plus ne font pas mystère de leur volonté [de devenir une grande puissance de demain], sans forcément que ce soit hostile à notre endroit »[88]. Cette formulation nous renvoie à la définition du contexte et de la menace : la notion de « guerre économique » est récusée au nom de l'état de compétition. La France n'aurait donc pas d'adversaires, encore moins d'ennemis, mais des concurrents. Elle promeut ainsi une lecture économique de la situation, non pas une lecture géopolitique.

Nous l'avons souligné supra, les Etats-Unis se distinguent par la cohérence de leur appareil de sécurité nationale. Cela se traduit par l'existence d'un système rôdé au sein duquel l'intégration sécurité nationale-sécurité économique est « naturelle » et parfaitement transposée sur le plan organisationnel. Elle mobilise des acteurs très expérimentés qui savent se montrer agressifs, et s'illustre par la coopération systémique entre SR et acteurs politiques et économiques. Ainsi s'affichent ensemble dans la conduite d'affaires contentieuses entre sociétés et pays concernés le *Department of Justice* (DoJ) avec le *Federal Bureau of Investigation* (FBI) et le *Department of War* (DoW) avec la *National Security Agency* (NSA) par exemple, soutenus en cela par l'exécutif mais aussi par le Congrès.

Ce système est également capable de s'adapter. À partir des années 2000-2010, les États-Unis ont compris que l'extraterritorialité du droit et le contrôle des transactions en dollars à l'échelle du globe, originellement utilisés dans le cadre de la *GWOT*, pouvaient constituer des instruments redoutables en matière de « guerre économique ». Face à l'affirmation chinoise, ils ont jugé qu'ils ne pouvaient pas y renoncer, et se sont donc lancés dans des entreprises de conquête très agressives. Pour la seule France, les exemples sont nombreux et retentissants. Les cas de Alstom Power et de BNP Paribas exposés ci-dessous sont emblématiques.

Le cas ALSTOM POWER

En situation délicate en 2003, Alstom voit son département « motorisation (Alstom Power) » être racheté par le géant américain General Electric en 2015, après une séquence d'intimidation et de captation-prédation orchestrée par les autorités américaines. Alstom a depuis racheté à grands frais une partie de la compétence « turbines », à l'exception toutefois des turbines Arabelle qui équipent des centrales nucléaires.

À travers l'affaire Alstom, et notamment le cas Pierucci, sont mises en relief plusieurs spécificités et pratiques américaines qui méritent notre attention, parmi lesquelles :
- **Le rôle du renseignement économique** dont la pratique est établie et parfaitement maîtrisée depuis des décennies. L'IE est partie intégrante du renseignement, la dimension économique étant un domaine d'intérêt national placé au cœur de la politique de puissance américaine ;
- **L'arsenalisation de la lutte contre la corruption** : les dispositifs FCPA servent aujourd'hui avant tout à protéger les entreprises américaines d'une concurrence potentiellement indue ou faussée. Il ne s'agit pas là d'un dispositif en réaction, mais au contraire d'une démarche proactive,

[87] Frédéric Pierucci, Témoignages à l'occasion des séminaires d'Aix-en-Provence et de Paris, *op. cit.*
[88] Céline Berthon, *Les Échos, op. cit.*

véritablement offensive. L'IE est utilisée pour « aller chercher » des cas, non pas pour analyser une éventuelle situation advenue. On notera par ailleurs que cette démarche comprend également un volet dissuasif que tout concurrent ne peut qu'ignorer à ses dépens : toute la puissance d'enquête, de contrôle et de rétorsion des États-Unis pèse en permanence sur tous les acteurs étrangers ;

- **L'intégration du monde économique, des services de renseignement et des sphères politiques et juridiques** : il s'agit là d'un fait remarquable que l'auteur de cette étude a pu relever dans sa pratique des institutions américaines dans ses fonctions passées au sein de la Mission de défense (MDD) de l'ambassade de France à Washington. Le travail en équipe, la primauté de l'intérêt national, la circulation de l'information, la cohérence des actions menées et le soutien mutuel sont un « trait culturel » qui se décline dans la pratique de manière redoutablement efficace. Dans ce cadre, l'association pleine et entière des services de renseignement à la démarche publique, y compris en matière juridique, est tout à fait ordinaire et assumée : pour un esprit américain, elle est même une évidence ;
- **L'esprit du modèle juridique et le « droit du plus fort »** : la culture de la négociation qui repose sur l'aveu est en fait un système implacable qui n'est jamais que le reflet de la puissance de l'autorité publique. Face aux capacités et à la détermination de ces autorités, qui ne cèderait pas ?

En outre, l'appareil américain est résolument intrusif et dissuasif. Les pénalités financières infligées sont une chose, la transparence exigée en est une autre, bien plus pernicieuse et dommageable à terme. En effet, l'administration américaine cherche à imposer au terme des négociations un contrôle par ses soins du respect par l'entreprise sanctionnée de ses obligations légales. Ainsi, elle rend ladite société « transparente » pendant un certain temps, décidé lors du prononcé du jugement, et peut donc bénéficier du savoir que celle-ci détient, ce en toute légalité, pour ensuite l'utiliser contre elle au besoin. Cette transparence imposée par la conformité est un instrument redoutable d'intelligence économique et un formidable levier dans le contexte de compétition économique que l'on connaît. C'est pourquoi la France s'est dotée d'instruments crédibles pour prendre cette mission à son compte et ainsi éviter l'entrisme américain (voir Partie 2, p. 60, Loi Sapin II). Par ailleurs, comme les cas exposés le démontrent, l'arsenal, la pratique et la détermination des autorités américaines exercent en permanence une pression sur les entreprises étrangères, en particulier celles qui sont cotées à la bourse de New York.

Le cas BNP Paribas

Ayant plaidé coupable devant la cour suprême de New York le 30 juin 2014, la banque se voyait condamner à une amende de près de $9 Mds pour avoir violé les embargos économiques américains à l'encontre de Cuba, de l'Iran et du Soudan entre 2002 et 2009. Les actions de la banque étaient légales en Europe, mais puisqu'elle avait utilisé des paiements en dollars via sa filiale à New York, elle est tombée sous le coup de la loi américaine[89]. Cette amende s'accompagnait d'une mise sous contrôle, dans le

[89] Toute opération financière effectuée en dollars doit être conforme à la réglementation américaine, même si elle est réalisée par une entreprise qui n'est pas américaine.

cadre des procédures dites de conformité, qui contraint l'entité ainsi condamnée à être placée sous contrôle d'autorités américaines pour une certaine durée, donc totalement vulnérable.

Qui plus est, cet écosystème dispose d'atouts considérables. En premier lieu, citons les capitaux : le dynamisme économique américain de manière générale, et en particulier celui de la *New Tech*, confère à Washington une arme de poids qu'est le capital disponible à l'investissement, soit sous la forme de prises de participations dans des sociétés ciblées, soit de rachats. Les entreprises américaines de la *New Tech* disposent ainsi d'une manne financière considérable – dont certains s'inquiètent d'ailleurs, y voyant une possible bulle financière dont l'éclatement pourrait causer des dégâts considérables à l'économie mondiale -, qui leur permet de s'imposer via la pression financière. Mais il ne s'agit là que d'un aspect du problème. En effet, les Etats-Unis, par l'imposition de nouvelles mesures coercitives (droits de douane) recherchent l'asymétrie de la dépendance et pour cela usent de mesures destinées à renforcer leur attractivité voire à l'imposer. De ce fait, les arsenaux défensifs mis en place par leurs « partenaires-concurrents » sont en partie contournés puisque certaines entreprises n'auront, économiquement parlant, d'autre choix que de s'installer aux Etats-Unis, via des filiales, pour profiter des conditions avantageuses offertes : c'est toute la logique qui sous-tendait le *Inflation Reduction Act* (IRA) de l'administration Biden[90]. Soulignons également les performances du cyber, un domaine de compétence singulière des Etats-Unis qui l'ont développé et façonné depuis trois décennies maintenant. Les GAFAM et l'écosystème associé sont redoutables, de même que les SR, comme l'a démontré le conflit Russie-Ukraine où les performances des armées ukrainiennes, lors de l'offensive initiale russe et depuis, s'expliquent en grande partie par la très grande qualité du renseignement américain, du niveau tactique au niveau stratégique, elle-même reposant sur des techniques cyber maîtrisées et sans doute à ce jour inégalées. Cette domination technologique permet la conquête de nouveaux marchés, y compris par la collecte permanente d'informations et la captation de données sensibles ou stratégiques, de manière directe ou indirecte via le US *Cloud Act* par exemple[91]. Elle s'articule en effet de multiples manières, notamment lors des procédures d'audit[92], avec le droit ou *lawfare*[93], un troisième instrument de puissance redoutable s'il en est, et une spécificité américaine, même si la Chine cherche à agir en miroir et commence à déployer des mesures dans ce domaine[94]. Il permet aux Etats-Unis d'exploiter leur position dominante pour imposer leur droit et leurs normes à des concurrents, fussent-ils des alliés, de manière brutale au besoin. Cette politique trouve ses fondements dans un arsenal législatif dont les présupposés sont parfaitement légitimes puisqu'il s'agit de lutter contre la corruption, notamment au sein des entreprises américaines. C'est ainsi que sera mis en place en 1977 le FCPA. Or, sous la présidence Clinton, en période d'hégémonie américaine, l'idée fait son chemin de recourir à cet instrument pour lutter contre la concurrence « déloyale » ; dès lors, de manière disproportionnée, la lutte anti-corruption va servir à affaiblir les concurrents étrangers et, avec le temps, à exporter le droit des affaires améicain et son corollaire, le principe de la négociation (deal, après aveu, sous forme de compensation financière) plutôt que

[90] U.S. Congress, « *Inflation Reduction Act of 2022 (IRA) : Provisions Related to Climate Change* », 16 août 2022, https://www.congress.gov/crs-product/R47262, consulté le 15 novembre 2025.
[91] *Cloud Act* du 23 mars 2018, *op. cit*.
[92] Séminaire du 28 janvier 2025, Paris, *op. cit*., Les procédures d'audit, très intrusives, permettent d'associer droit et cyber et d'étendre les recherches à l'ensemble de la chaîne des sous-traitants de l'entreprise auditée, la rendant ainsi plus vulnérable à terme.
[93] On trouvera de nombreuses études sur le *Lawfare* sur le site de l'EGE par exemple, et des recommandations formulées pour y faire face dans les rapports précités.
[94] Il s'agit de la récente initiative chinoise d'octobre 2025 portant sur le contrôle des terres rares, notamment analysée par Arnaud de Nanteuil, *La Chine durcit le contrôle de ses terres rares : un nouveau levier d'influence ?*, Le club des juristes, 22 octobre 2025.

celui de la défense[95]. Ces pratiques ont conduit la France à promulguer la loi dite Sapin II et à mobiliser le Parquet national financier (PNF), lequel toutefois, en matière économique, tendrait selon certains experts à importer les pratiques américaines et à favoriser la négociation en cas de contentieux[96]. L'ingérence par le droit recourt à de nombreux outils dont le mécanisme ITAR est un exemple aussi connu que redouté, d'autant plus qu'il est, sinon juridiquement, du moins dans la pratique, en quelque sorte rétroactif[97]. Par ce dispositif, les Etats-Unis s'octroient la possibilité d'exercer un droit de regard sur toute exportation ou transfert d'arme ou de technologie entre pays tiers à partir du moment où un simple composant est d'origine américaine. Cet outil leur permet non seulement de contrôler des marchés et des transactions, mais aussi, comme le rappelle la Délégation parlementaire au renseignement (DPR), d'obtenir une visibilité sur des matériels sensibles, ce qui procure évidement à terme un avantage compétitif aux entreprises américaines concernées[98]. Comme le constate le PNF, la compétence territoriale américaine s'est élargie avec le temps, est interprétée de manière extensive (la présomption d'intention corruptrice est retenue dans tous les cas où le contexte de l'infraction indique une forte probabilité de destination frauduleuse des fonds), la responsabilité des personnes morales est élargie et les sanctions financières assorties d'un programme de mise en conformité[99].

Enfin, aujourd'hui, sous pression américaine d'ailleurs, notons que les initiatives de l'UE en matière de sécurité-défense se déclinent sous la forme de lourds investissements financiers et programmes d'armement qui captent l'attention de Washington. Les autorités politiques et les principaux acteurs économiques outre-Atlantique ne cachent pas leur ambition de bénéficier des fonds européens (Programme européen pour l'industrie de la défense-EDIP notamment) au profit de la revitalisation de leur propre base industrielle de défense, ni d'établir des partenariats dans une logique de co-production voire de co-développement entre entreprises américaines et européennes pour compenser les insuffisances de la BITD américaine et se replacer en situation de supériorité technologique dans certains secteurs clés[100]. C'est donc un nouveau chantier de coopération et de compétition entre partenaires-concurrents qui s'ouvre.

La République populaire de Chine (RPC) : une puissance de plus en plus agressive

Les autorités chinoises voient dans la sécurité économique un contributeur essentiel à la sécurité nationale, elle-même à comprendre comme une sécurité politique au sens où sa mission première est d'assurer la pérennité du régime (« Faire de la sécurité politique la priorité absolue »)[101]. Pour cela, Pékin a mis en place un arsenal de dispositifs au fil du temps qu'il n'a eu de cesse de consolider et de formaliser. C'est en effet en mars 1986 qu'est élaboré le Plan 863 de rattrapage technologique via le développement d'un écosystème d'innovation combinant universités, centres de recherche militaires

---

[95] Mme Sophie Scemla, cabinet Gide, « Les entreprises françaises face aux services de renseignement étrangers », *op. cit.*

[96] *Ibid.*

[97] M. Dupré, SISSE, entretien du 10 septembre 2025. On parle de « rétroactivité » dans la mesure où le classement, après coup, d'un composant ou d'une donnée technique déjà exporté sur la liste USML peut conduire à traiter l'opération comme ayant toujours relevé de l'ITAR, faisant ainsi surgir un risque de violation.

[98] DPR, rapport d'activité 2022-2023, op. cit. : « L'administration américaine s'en est prévalue pour bloquer en 2018 l'exportation de missiles SCALP et MBDA vers l'Égypte au motif de la présence d'une puce électronique américaine. Au cœur du contrat de vente de 24 *Rafales* supplémentaires pour un montant de deux milliards d'euros, les missiles SCALP ont finalement pu être livrés, mais avec un retard important suite à l'intégration d'un composant analogue par MBDA ».

[99] Jean-François Bohnert, procureur de la République financier, audition à l'Assemblée nationale, 9 février 2023.

[100] Hélène Masson, Nicole Viboux et Didier Gros, *Les limites et les vulnérabilités de l'industrie de défense américaine*, Rapport N°7, Observatoire de la politique de défense américaine, Fondation pour la recherche stratégique, octobre 2025, p. 68.

[101] Mathieu Duchâtel, *Stratégie de sécurité nationale de la Chine : une lecture du nouveau Livre blanc*, Institut Montaigne, 14 mai 2025.

et civils, et entreprises[102]. L'idée a consisté depuis à se développer et à innover tout en captant les données et savoir-faire étrangers, et en protégeant très efficacement les secteurs critiques chinois[103]. Le plan *Made in China* 2025, qui vise à réduire la dépendance par rapport à l'Occident dans le domaine technologique à 30% des technologies, en est le dernier avatar. Nous retiendrons, comme références :

La « *Comprehensive National Security* » de 2014 qui, pour la première fois, expose les ambitions chinoises dans le contexte de l'intensification de la compétition stratégique internationale, fixe un objectif national de « méga-sécurité » et définit cinq fonctions essentielles : la sécurité du peuple, l'objectif ultime ; la sécurité politique, la tâche fondamentale ; la sécurité économique, la fondation ; la sécurité militaire, scientifique et technologique, culturelle et sociétale comme moyen de garantie ; la promotion de la sécurité internationale comme soutien.[104]

Un arsenal législatif mis en place entre 2014 et 2017, au moment où les tensions se sont accrues entre Chine et Etats-Unis, ces derniers, sous la présidence Obama, ayant annoncé le « pivot vers l'Asie » pour faire face à l'affirmation de la puissance chinoise. Cet arsenal comprend notamment les lois sur le contre-espionnage (2014), la loi sur la sécurité nationale (2015) qui fait de l'intégration civilo-militaire (ICM) une stratégie nationale, la loi sur les organisations non gouvernementales étrangères (2016) et les lois sur la cybersécurité (2016).

La priorité donnée à l'intégration civilo-militaire (ICM) par la loi du 28 juin 2017 sur le renseignement national qui contraint légalement tout citoyen ou toute entreprise à participer à la collecte de renseignement, aussi bien à l'étranger que sur le sol national[105]. Comme le souligne la DPR, « Cette disposition fait de tout ressortissant chinois un potentiel espion »[106], et permet au Parti communiste chinois (PCC) de s'appuyer sur la diaspora chinoise au travers des réseaux d'associations, d'étudiants, ou de commerçants. Soulignons que le Comité de coordination et de développement de l'ICM est présidé par Xi Jinping lui-même[107]. Concrètement, l'ICM se déploie jusqu'au niveau municipal et utilise un certain nombre de leviers dont les fonds injectés dans les entreprises, les alliances entre industries, centres de recherche et départements des armées, ainsi que des zones dites de démonstration de l'ICM restructurées sous la forme de « *mega clusters* » (*clusters* dans le domaine maritime et naval par exemple, initiés par Hu Jintao)[108].

Le « Livre Blanc de 2025 » qui met en relief le concept holistique de sécurité nationale et annonce une possible stratégie de sécurité nationale qui couvrirait la période 2025-2030[109]. Ce document reprend le « narratif » usuel et affirme que « 5000 ans de civilisation ininterrompue confèrent à la nation chinoise une riche et profonde culture stratégique de sécurité nationale ». Le « concept de sécurité nationale globale » de Xi est donc la continuation naturelle de cette longue tradition, au service de la

[102] Antoine Bondaz, « Les entreprises françaises face aux services de renseignement chinois », *op. cit.*
[103] Jake Sullivan, ancien National Security Advisor sous l'administration Biden, a utilisé la métaphore du « *small yard, high fence* » (« petite cour, haute clôture ») pour décrire l'ambition américaine de contrôler et protéger un périmètre restreint de technologies stratégiques.
[104] Gouvernement de Hong Kong, « *A holistic approach to national security* », National Security Education Day, https://www.nsed.gov.hk/national_security/index.php?l=en&a=safety, consulté le 15 novembre 2025.
[105] Antoine Bondaz, « Un tournant pour l'intégration civilo-militaire en Chine », *Recherches et documents*, N° 07/2017, FRS, octobre 2017. La loi précise dans son article 7 que « *toute organisation ou citoyen doit soutenir, assister et coopérer avec les activités liées au renseignement national* ».
[106] DPR, rapport d'activité 2022-2023, *op. cit.*
[107] Antoine Bondaz, *op. cit*.
[108] *Ibid*.
[109] Bureau d'information du Conseil des affaires d'État de la République populaire de Chine, *La sécurité nationale de la Chine dans la nouvelle ère*, 12 mai 2025 (traduction à partir du communiqué de l'Agence de presse Xinhua).

modernisation aux caractéristiques chinoises, dans la recherche d'un équilibre entre les objectifs de sécurité nationale et les objectifs de développement intérieur.

La dimension expansive du concept de sécurité nationale est désormais assumée, en ces termes : « La sécurité nationale de la Chine à l'ère nouvelle est une sécurité globale, systématique et d'envergure. Elle privilégie la sécurité du peuple, repose fondamentalement sur la sécurité politique et adhère aux principes des intérêts nationaux »[110]. Sont ainsi coordonnés le développement et la sécurité, la sécurité extérieure et intérieure, la sécurité territoriale et nationale, la sécurité traditionnelle et non traditionnelle.

Cela conduit aujourd'hui les experts occidentaux à évoquer un phénomène dit de « *securitization of everything* »[111], dont on ne peut manquer de noter qu'il se rapproche, dans sa logique, de la démarche américaine.

Sur le plan de la sécurité économique, la puissance chinoise s'appuie donc d'abord sur une synergie nationale qui combine les actions d'entreprises chinoises, tout à fait capables d'initiative dans ce domaine[112], et que le régime laisse agir dans l'univers de la compétition internationale jusqu'au moment où il estime devoir intervenir, sur les manœuvres de services de renseignement particulièrement puissants, omniprésents et offensifs, totalement intégrés à la hiérarchie politique sans distinction du domaine privé ou public, mais aussi sur l'activisme d'une population mobilisée, de gré ou de force, notamment à l'étranger (cas de la diaspora) et, enfin, sur la matrice d'un régime de contrôle de nature totalitaire sous l'autorité du PCC. Elle entretient également un système opaque : pénétrer les arcanes du monde politico-administratif et économique chinois est particulièrement difficile, ce qui confère à la Chine un atout substantiel dont elle use et abuse. Sur ce plan, l'enjeu consiste à prévenir une intégration horizontale et verticale des capacités chinoises en essayant d'identifier les utilisateurs finaux des technologies autour desquelles existe une coopération, en particulier lorsqu'elles sont potentiellement duales[113]. Ce système recourt à des méthodes très variées (espionnage classique, pas seulement du fait des services ; mobilisation de capitaux ; exploitation des fonds européens[114] ; instrument de la dette ; accaparement et contrôle d'infrastructures stratégiques dont aéroports et ports ; attaques réputationnelles ; submersion par l'offre via l'écoulement d'une surproduction nationale ciblée[115]) et dispose de moyens d'envergure. Ainsi, sur le plan financier, la puissance chinoise est redoutable. La masse de liquidités dont elle dispose lui permet évidemment d'exercer une pression capitalistique sur des entreprises stratégiques ciblées[116], mais aussi, et c'est un de ses modes d'action privilégiés, de séduire et d'attirer, c'est-à-dire de corrompre responsables et experts politiques, économiques ou scientifiques en offrant des conditions de rémunération ou de

[110] *Ibid*. (avant-propos).
[111] Katja Drinhausen et Helena Legarda, *op. cit*. La Chine se défend évidemment de « tout sécuriser ».
[112] Paul Charon, entretien du 9 septembre 2025, IRSEM. Le régime conserve la possibilité de mettre la main sur toute action ou initiative des entreprises chinoises.
[113] Antoine Bondaz, *op. cit*. L'intégration horizontale peut se faire par le rachat d'entreprises dans un secteur donné, et l'intégration verticale sera le résultat de la captation de données et de compétences ainsi effectuée au profit d'une filière industrielle alors modernisée et capable de rivaliser avec les concurrents occidentaux.
[114] Nicolas Ravailhe, entretien du 27 octobre 2025 : plutôt que d'espionner, la Chine capte l'argent qui se trouve dans les fonds européens, et exploite les bases de données de l'UE, largement ouvertes (avec le dessein, de la part de certains pays européens, d'encourager les échanges). C'est ainsi que le guide du *Cooperation Program* 4 de l'UE qui porte sur l'innovation est accessible à la Chine.
[115] Voir le cas emblématique des voitures électriques chinoises en Europe.
[116] DPR, rapport d'activité 2022-2023 : « dispose de liquidités inégalées qui lui permettent à la fois d'investir des sommes colossales dans des projets porteurs (innovation et rattrapage technologique) et de conquérir des marchés ou parts de marchés, notamment dans les secteurs stratégiques (rachat d'entreprise ou participation au capital) ».

travail sans égales[117]. Selon la DPR, la France est particulièrement exposée dans les domaines des biotechnologies, des secteurs à la technologie duale, et subit les assauts capitalistiques (*Private Equity* et *Venture Capital*) contre ses start-ups ou « PME spécialisées dans les technologies de rupture (calcul quantique, science de la donnée) »[118]. Ces actions touchent également le monde de l'université et des centres ou laboratoires de recherche dont on sait qu'ils sont souvent en état de dépendance financière d'une part, et encore insuffisamment sensibilisés au risque d'ingérence d'autre part. Sont également à l'œuvre les services de renseignement, dont on retiendra qu'ils constituent un levier stratégique de puissance au service de la sécurité du régime, de la continuité du PCC, de la montée en puissance de l'État, de la réunification de Taïwan et de la compétition systémique avec l'Occident[119]. Si, sur le plan doctrinal, l'affichage, dans la grande tradition communiste, est défensif (préservation de la révolution face aux « agresseurs capitalistes et impérialistes »), la pratique est résolument offensive et recourt à des méthodes dites hybrides (vision intégrée de la sécurité) où se chevauchent et se recoupent guerre et paix, intérieur et extérieur, civil et militaire. Aujourd'hui, dans le contexte d'intense compétition économique et politique, le renseignement chinois met l'accent sur l'accès à l'information conçue comme une arme offensive intégrée aux nouvelles technologies, y compris dans le domaine cognitif[120]. Enfin, de plus en plus, la Chine se dévoile et « tombe le masque », obsédée par sa volonté de rattrapage et en particulier par son « retard » en matière de recherche fondamentale. Après avoir pendant environ 25 ans organisé son rattrapage économique et technologique selon une approche méthodique et discrète, assortie de discours lénifiants à l'attention de ses concurrents occidentaux, elle agit désormais de manière plus ouverte, désinhibée et agressive (on se souviendra de la période Covid et de ce que le MEAE, reprenant la thèse de l'IRSEM, avait qualifié de « russianisation » des méthodes chinoises), et déploie des dispositifs en miroir de la partie américaine. En témoignent les répliques brutales aux droits de douane sous forme de coercition (restriction des exportations de terres rares en octobre 2025[121]), les mesures nouvelles de *lawfare* promouvant l'extraterritorialité des lois chinoises ou encore les efforts intensifiés en matière de normalisation au sein des organisations internationales[122].

Le cas Ligeance Aerospace Technology Co Ltd

Cette société chinoise possédée par la Sichuan Development Holding est spécialisée dans la fabrication de composants aéronautiques. Elle a acquis en 2017 le groupe britannique Gardner Aerospace dont une des sociétés est basée en Ardèche (Mazères), et opère en tant que sous-traitant du groupe aéronautique de rang 1 Gardner. Or, Ligeance Aerospace est liée à la BITD chinoise et travaille à son profit sur des technologies nécessaires notamment à la fabrication des moteurs WS-15 de l'avion de chasse furtif J-20. Le moteur WS-15 de 4ème génération serait comparable au moteur F-119 qui équipe le F-22 américain. Par ces rachats, la Chine a pu capter des technologies ou savoir-faire qui lui permettent aujourd'hui d'intégrer sa chaîne de valeur à partir du rhénium (métal très réfractaire

[117] Information non attribuable

[118] DPR, *op. cit.*

[119] Marine Dayma, *La doctrine de renseignement chinoise. De la surveillance à l'armement du renseignement : une analyse de la doctrine*, Mémoire de fin d'études, Mastère renseignement 2023-2024, IEP d'Aix-en-Provence, 2025, p. 5.

[120] *Ibid*.

[121] Arnaud de Nanteuil, Club des juristes, op. cit.

[122] À l'image de la pression exercée par la Chine sur l'OMC à l'occasion de la crise de la Covid-19.

indispensable aux alliages) d'une part, et de procéder à une intégration horizontale et verticale d'autre part, au profit des capacités modernisées de ses équipements militaires[123].

Des acteurs secondaires aux ambitions affirmées et aux méthodes intrusives

La Russie et sa puissance de nuisance : dans l'espace public, au sein des médias, la Russie est systématiquement présentée comme une menace en tous domaines, et souvent mise sur pied d'égalité avec la Chine en particulier. Or, la réalité est plus complexe. La Russie, puissance résurgente, ne cache pas son hostilité envers l'Occident et manœuvre au quotidien en ce sens. La menace qu'elle représente en bien des domaines est incontestable. Pour autant, elle est hétérogène et dissymétrique, notamment sur le plan économique à notre encontre, et constitue en l'état plus l'expression, selon diverses modalités, d'une capacité de nuisance que d'une véritable stratégie de conquête. En effet, les relations économiques entre la Russie et la France sont, surtout depuis 2022, extrêmement réduites et n'offrent donc pas, par construction, une surface de contact suffisamment large pour permettre la mise en œuvre d'une telle stratégie. Les services français et les administrations en charge sont unanimes : sur le plan économique, la menace russe est secondaire, même si ses opérations hostiles à l'encontre d'entreprises de la BITD demeurent préoccupantes. Parmi ses procédés d'exécution, on relèvera la cooptation d'élites (politiques, économiques), le recours permanent à l'arme cyber[124] et des mesures de rétorsion aux sanctions qu'elle subit[125].

Les partenaires européens et le cas allemand : une concurrence entre alliés de plus en plus désinhibée

Le SGDSN, les SR comme le SISSE partagent leur analyse sur la menace croissante que posent certains partenaires et alliés au sein de l'UE depuis deux à trois ans, tout particulièrement l'Allemagne, mais aussi l'Italie ou les Pays-Bas, indépendamment du cas de la concurrence toujours vive exercée par le Royaume-Uni.

Nous nous attarderons ici sur le cas allemand, emblématique à bien des égards de l'ambiguïté de la relation stratégique franco-allemande, des divergences d'approche en matière économique, et des effets et conséquences du durcissement de la compétition économique internationale.

L'Allemagne est en effet passée maître dans l'art de capter les fonds européens afin d'accroître ses capacités de production et d'asseoir sa compétitivité sur le marché mondial. Comme le constate Nicolas Ravailhe, « elle contrôle ainsi aujourd'hui des pans entiers de l'économie d'États européens et donc des intérêts politico-économiques de l'UE »[126], et ses excédents commerciaux sont considérables.

Confrontée à de très graves difficultés sur le plan énergétique depuis son abandon du nucléaire en 2011 et l'échec total, sous la contrainte de la guerre en Ukraine, de sa stratégie de compensation par dépendance vis-à-vis de la Russie entretemps, l'Allemagne produit depuis de considérables efforts dans le secteur des énergies dites renouvelables et cherche à s'imposer face à la concurrence d'autres modèles. À l'encontre de la France, sa démarche aura été radicale : éliminer l'avantage comparatif exceptionnel français en matière énergétique via la déstabilisation de sa filière nucléaire. Pour y parvenir, elle n'aura pas hésité à recourir à des fondations politiques financées par le gouvernement fédéral, des instruments de lobbying, telles que la *Heinrich Böll Stiftung,* rattachée à *Die Grünen,*

[123] Antoine Bondaz, *op. cit.*

[124] ANSSI-CERT-FR, *Panorama de la cybermenace 2024*, 11 mars 2025.

[125] Maxime Audinet, IRSEM, entretien du 9 septembre 2025 : certaines entreprises françaises toujours présentes en Russie, dont Auchan qui parie sur la levée prochaine des sanctions, sont soumises à des pressions et menaces de rachat, par Gazprombank en l'occurrence.

[126] Nicolas Ravailhe, « L'Europe favorise la course à la domination entre ses membres », *L'Audace*, N°1, 2025, p. 28.

insérée dans le *Réseau Action Climat* et active auprès d'*Europe Ecologie Les Verts (EELV)*[127]. Par la mobilisation des acteurs politiques écologistes des deux côtés du Rhin et le soutien apporté à des organisations non gouvernementales (ONG) activistes dont *Transparency International*, mais aussi par l'exploitation des divisions politiques françaises et l'absence d'une vision stratégique hexagonale digne de ce nom en la matière, l'Allemagne est parvenue à affaiblir considérablement notre filière nucléaire, au point qu'il aura fallu attendre d'être en quelque sorte au bord du précipice pour que la direction politique du pays réagisse enfin. Une combinaison de naïveté, parfois sous-tendue par un européisme pathologique, de complicité passive ou active et d'incohérence stratégique a offert une opportunité historique à notre allié d'outre-Rhin.

Mais plus largement, le *zeitenwende* allemand, nonobstant les difficultés économiques actuelles, va se décliner en bien d'autres domaines, notamment, car c'est un objectif national clairement affiché, la sécurité-défense, et ne manquera pas d'exercer une pression concurrentielle croissante sur les actifs et le potentiel français dans des filières stratégiques (énergie toujours, défense, spatial, aéronautique, etc.)[128]. Pour ce faire, l'Allemagne dispose de plusieurs atouts, outils ou méthodes. Il s'agit en premier lieu de la robustesse de son écosystème industriel manufacturier qui représente près de 21% de son PIB en 2023[129] et fait preuve d'excellence dans plusieurs secteurs tels que « la mobilité, la mécanique, la chimie et le pharmaceutique, l'électrotechnique et l'agroalimentaire »[130]. Par ailleurs, l'attractivité de son réseau industriel lui permet de nouer des partenariats, avec les États-Unis notamment, dans le domaine de la sécurité-défense qui renforceront sa position de leader ou coleader dans différents secteurs de pointe, potentiellement au détriment de l'industrie française[131]. Soulignons ensuite sa politique d'investissements massifs, grâce à une situation financière malgré tout plus saine qu'en France, dans des secteurs de pointe, selon une stratégie offensive plus que défensive qui vise à conquérir des parts de marché dans le « grand jeu » international, non pas en soutien à l'affirmation géopolitique de l'Union européenne mais à des fins de développement économique national. L'exemple du spatial, un domaine d'excellence français, est parlant : « Berlin en a fait une vraie priorité à l'image de Paris, mais contrairement à la France, l'Allemagne y met vraiment beaucoup de moyens financiers. Fin septembre, le ministre de la Défense allemand Boris Pistorius a promis une enveloppe budgétaire de 35 milliards d'euros dans des projets militaires spatiaux défensifs et offensifs d'ici à 2030, dont une constellation qui pourrait même mettre gravement en danger la constellation européenne IRIS, fortement défendue par la France » [132]. Attardons-nous enfin sur un cas d'école récent qui illustre parfaitement le niveau d'agressivité de l'Allemagne :

---

[127] EGE, *Ingérence des fondations politiques allemandes & sabotage de la filière nucléaire française*, rapport d'alerte, juin 2023.

[128] Liesa Johannssen, « Défense : l'Allemagne annonce plusieurs centaines de milliards d'euros d'investissements », *La Tribune*, 4 mars 2025.

[129] DGT, *Allemagne : indicateurs et conjoncture*, 30 avril 2024. Cela représente 21% d'un PIB de 4121 Mds d'euros. Pour mémoire, l'écart avec la France, dont le PIB est en 2024 de 2917 Mds d'euros en valeur, et la part de l'industrie de 11% à peine, est abyssal.

[130] CCI France International, *Le secteur industriel en Allemagne*, 20 février 2024, **https://www.ccifrance-international.org/le-kiosque/notes-sectorielles/n/le-secteur-industriel-en-allemagne.html**, consulté le 4 décembre 2025.

[131] Les récents accords de partenariat entre Rheinmetall et Anduril (missiles Barracuda et drones par exemple) témoignent d'une dynamique engagée outre-Rhin qui pourrait à terme représenter une concurrence redoutable pour les industries françaises.

[132] Michel Cabirol, « Comment l'Allemagne va mettre K-O la France dans le spatial », *La Tribune*, 10 novembre 2025. La France a quant à elle annoncé le 12 novembre 2025 une hausse du budget spatial à 10,2 Mds d'euros d'ici 2030.

Le cas de la pépite française Ternwaves

Spécialisée dans le domaine de la communication satellitaire aux enjeux civils et militaires, elle a mis au point une technologie de connectivité révolutionnaire pour les réseaux IoT satellitaires, et a été sélectionnée par les opérateurs européens du spatial en raison de la qualité de son savoir et de ses produits[133]. Nos partenaires-concurrents d'outre-Rhin se sont efforcés de remettre en cause ce choix et ont utilisé un arsenal de moyens pour délégitimer l'offre française en accusant l'entreprise de contrefaçon. Pour y parvenir, c'est la Bundeswehr qui a, en coopération avec les services de renseignement, activé ses réseaux aux Etats-Unis et mobilisé le *U.S. Patent and Trademark Office* (USPTO) pour attaquer la start-up et faire en sorte que son accréditation par les autorités américaines soit rejetée[134]. La procédure aura duré environ un an et coûté 200 000 dollars à Ternwaves, une somme considérable pour la jeune pousse. La perte de temps subie, les dépenses occasionnées et la fragilisation par attaque réputationnelle se sont ainsi combinées pour tenter de faire tomber un concurrent, via des instruments extra-européens, en l'occurrence ceux du grand allié commun.

Les partenaires du Proche Moyen-Orient (PMO) et la Turquie : des « concurrents » décomplexés

Ces puissances moyennes en voie d'affirmation sur le plan géoéconomique, principalement l'Arabie saoudite, les Émirats arabes unis (EAU), Israël ou encore la Turquie, cherchent à diversifier leurs partenariats et à accéder à des parts de marché dans des domaines de plus en plus variés, incluant celui de la sécurité-défense. La maîtrise de la cybernétique et des nouvelles technologies liées à l'IA ou au quantique sont un exemple emblématique des objectifs affichés par les pays du PMO. Les accords passés par l'Administration Trump au printemps 2025 avec l'Arabie saoudite et les EAU portant sur des investissements colossaux dans le domaine cyber et IA en sont l'expression concrète[135]. Quant à Israël, ses investissements dans les nouvelles technologies, bien au-delà d'ailleurs du seul domaine de la sécurité-défense (technologies de désalinisation, filtration et purification des eaux par exemple), lui confèrent désormais un rôle de tout premier plan à l'échelle internationale et en font un des leaders du marché dont la compétence technique est reconnue voire enviée. La Turquie, enfin, désormais concurrentielle sur une large gamme de produits défense de rang technologique intermédiaire, présente une menace plus classique de rattrapage par différents moyens, dont l'espionnage.

Dès lors, ces acteurs sont pour la France des concurrents de plus en plus redoutables, soit par leur niveau de compétence (Israël), soit par leur puissance financière (monarchies du Golfe), soit par leur appétit de développement et de conquête des marchés (Turquie). Or, là encore, la France est placée face à un dilemme : comment attirer des fonds indispensables à son maintien dans la compétition internationale de haut niveau sans se rendre vulnérable à terme ? Sa politique d'attractivité économique invite en effet les puissances du Golfe à investir, notamment dans des start-ups en demande de fonds, mais elle présente en retour des risques puisque ces investissements sont l'occasion pour les pays en question d'accéder à des savoirs (identification des chercheurs) ou d'exercer ensuite une pression sur ces chercheurs ou les dirigeants des sociétés concernées (tentatives de débauchage par exemple). Nos services ne parlent pas dans ce cas d'ingérence en tant que telle, mais d'un risque désormais systémique directement lié à nos propres insuffisances, notamment sur le plan financier, qu'il convient de gérer dans la durée. Quant à la compétition avec Israël, elle se joue dans

[133] Julie Duclercq, « Les entreprises françaises face aux services de renseignement étrangers », Paris, *op. cit*.
[134] *Ibid.*
[135] A l'occasion de la visite d'État du président Trump en mai 2025, des annonces d'investissements colossaux par l'Arabie saoudite et les EAU ont été faites, de l'ordre de $600 Mds pour la première et de $200 Mds pour les seconds.

des secteurs de haut niveau technologique où des coopérations pourraient être mutuellement bénéfiques, au prix d'une captation réciproque de savoirs à gérer de part et d'autre.

Les voies et moyens

Il existe différentes manières de classer et de hiérarchiser les différentes catégories de menaces qui représentent chacune un ensemble de méthodes ou de moyens mis en œuvre dans le but de défendre ou promouvoir ses intérêts, jusqu'à l'ingérence. Comme vu précédemment, le canevas-type suivant peut servir de référence :

- Capitalistique
- Humaine
- Physique
- Technique (dont cyber)
- Juridique (*lawfare*)
- Réputationnelle
- Logistique (cas des chaînes d'approvisionnement)

Parmi les différents modes d'action mis en œuvre, on pourra mettre en relief :

- La captation des données qui va consister à mobiliser différentes techniques dont l'espionnage physique classique, l'intrusion cyber, le pillage, le recours à des contrats économiques déséquilibrés, etc. ;
- L'entrave, sous différentes formes, dont le *Lawfare*, les attaques cyber, le boycott, les poursuites judiciaires ou encore les attaques réputationnelles ;
- La coercition économique, sous la forme de politiques d'endettement massif (création de dépendances), d'exploitation d'asymétries globales (contrôle des flux des chaînes d'approvisionnement), d'imposition de droits de douane, de gels d'avoirs, d'embargos, etc. ;
- L'influence, qui peut se manifester par différents canaux (politique, diplomatique, recours à des ONG), et concerne en particulier l'imposition de normes internationales, la désinformation, la corruption, la cooptation d'élites et le débauchage (chercheurs, responsables politiques, etc.).

Étude de cas et rôle déterminant des services de renseignement

Le cas Eutelsat

La société Eutelsat est un concurrent direct de Starlink impliqué dans le projet européen IRIS. Après avoir fusionné avec *OneWeb*, pour conserver sa licence attribuée par la *Federal Communications Commission* (FCC), l'autorité de régulation des télécommunications aux Etats-Unis, un marché incontournable pour elle, Eutelsat s'est alors trouvée soumise aux exigences juridiques américaines, c'est-à-dire enjointe de signer une *Letter of Agreement* (LoA) avec l'administration. En la matière, il s'agit officiellement de protéger les infrastructures de télécommunications américaines, qu'Eutelsat pourrait fragiliser s'il ne satisfaisait pas à tous les critères de sécurité imposés aux autres opérateurs américains et étrangers. Bien évidemment, derrière cet objectif légitime se dissimule une stratégie d'accès aux données les plus sensibles d'un concurrent rendu « transparent » par les obligations imposées par la LoA. Dans un contexte marqué par la proximité du dirigeant de Starlink, Elon Musk, avec l'administration Trump, d 'une démarche originelle vertueuse, on passe ainsi à une démarche potentiellement hostile. Celle-ci se traduit par :

- La présence d'un officier de sécurité américain, ayant un accès direct au COMEX de l'entreprise, qui peut donc, en tant que citoyen américain, résidant aux Etats-Unis, être justiciable aux Etats-Unis ;

- L'imposition d'un registre PII (*Personally Indentifiable Information*), équivalent d'un ESTA, pour tout membre d'Eutelsat pouvant avoir accès à des informations en provenance des Etats-Unis, soit, dans les faits, l'obligation pour Eutelsat de fournir la liste de la quasi-intégralité de son personnel (donc son organigramme) à son partenaire-concurrent. D'éventuelles opérations de débauchage en seront facilitées ;

- L'obligation de fournir la liste des équipements principaux (*Principal Equipment*-PE) de l'entreprise avec les références techniques. Là encore, cela peut permettre à l'administration américaines d'interdire certains de ces équipements, pour des raisons techniques, au profit des leurs.

Eutelsat bénéficie d'un accompagnement par l'administration française (SGDSN, DGE, SISSE, ANSSI, DRSD) qui a évoqué un possible emploi de l'article 44 de la LoA dans lequel est stipulé qu'une entreprise française ne peut être « hors la loi » et doit respecter les différentes règlementations ou codes de l'administration française, en référence à l'article 40 de la loi de blocage. Or, dans les faits, la partie américaine ne respecte pas nos outils et maintient sa pression. La France et Eutelsat ont convenu en l'espèce de ne pas activer l'article 40 car les risques pour Eutelsat, dont près de 10% du CA se fait aux Etats-Unis, étaient trop élevés en cas de représailles.

Enfin, notons la pratique de l'audit américain combinant *lawfare* et cyber d'une part, Department of Justice (DoJ) et Department of War (DoW) (dont services de renseignement) d'autre part, via des prestataires inféodés et imposés, en l'occurrence la société Kroll[137], pourtant initialement rejetée par Eutelsat qui proposait une alternative française reconnue par l'administration américaine, qui laisse peu de doute quant aux conclusions de l'audit.

Des enseignements sont donc à tirer de cette situation appelée à se reproduire contre les entreprises françaises :

- Systématiser en France voire dans l'UE le procédé de la LoA, à l'instar des lettres d'engagement fixant les conditions d'exécution d'investissement en France, qui sert à protéger son écosystème ;

- Renforcer les mesures de sélection et de filtrage (*screening*) des ressources humaines afin de se prémunir contre des angles d'attaque liés par exemple à des doubles nationalités potentiellement problématiques ;

- Apprendre à fonctionner avec des « *shadow cabinets* » qui permettent de contourner la présence américaine en l'occurrence ;

- Développer des compétences nationales en matière d'audit afin d'éviter que soient systématiquement choisies des sociétés étrangères ;

- Sensibiliser le personnel des entreprises, mais aussi au sein des écoles de formation, sur la réalité de la concurrence ;

- Établir des Zones à Régime Restrictif (ZRR) au sein des établissement afin d'accroître le contrôle sur les auditeurs ;

- Constituer une base de données « retour d'expérience » (RETEX) au sein de l'administration française dont pourraient bénéficier d'autres entreprises.

[137]Kroll, https://www.kroll.com/en/services/financial-services-compliance-and-regulation/uk-regulation/financial-services-internal-audit, consulté le 10 décembre 2025.

Identification des tendances et des risques

Globalement, selon la communauté du renseignement, la principale menace, stabilisée à haut niveau, est d'ordre capitalistique. Les autres se répartissent à proportion à peu près égale, même si, malgré les efforts significatifs fournis depuis des années, la cybermenace est en légère progression, à la faveur notamment de la confusion croissante entre réseaux privés et publics, source d'extrême fragilisation[138].

La menace capitalistique est l'arme par excellence des Etats-Unis, mais aussi de la Chine et des pétromonarchies du Golfe, parfois sur invitation. Elle est favorisée aujourd'hui par le contexte économique lié à l'essor des nouvelles technologies qui voit émerger ou se consolider une multitude de start-ups ou de géants de la *New Tech* (IA, quantique, robotique, biotechnologies, etc.) dotés de moyens financiers considérables et donc d'une force de frappe à laquelle il est extrêmement difficile de résister. Ainsi, la puissance financière couplée à l'avance technologique rend le champ de la compétition particulièrement exigeant et limite considérablement les possibilités de protection.

Par ailleurs, la menace d'ordre réputationnel est désormais significative, concrétisée par le phénomène de *business disinformation* qui consiste par exemple à propager des rumeurs sur l'état d'une société ou d'un équipement afin d'éroder la crédibilité de l'acteur en question[139]. On mentionnera entre autres cas la désinformation chinoise concernant les capacités du Rafale à la suite des incidents entre l'Inde et la Pakistan, relayée par d'autres acteurs dans le but évident de nuire à l'industrie française en compétition avec de nombreux autres constructeurs sur des marchés prometteurs[140]. Dans le même registre, citons les récentes attaques réputationnelles contre Naval Group : des hackers ont prétendu cet été avoir soutiré un téraoctet de données sensibles à l'entreprise concernant les systèmes de gestion de combat des frégates FREMM et FDI, ainsi que ceux du SNLE *Le Vigilant*. Or, il s'avère qu'il s'agirait là non pas d'une attaque cyber mais d'une désinformation visant à entamer la crédibilité de l'entreprise[141].

D'autres procédés relèvent de la « coercition économique », sous différentes formes, les unes en apparence bénignes, telles que les mesures de *re-shoring* déployées par les États-Unis pour attirer des entreprises étrangères sur leur sol (cas des mesures d'incitation de la loi dite IRA sous Biden), les autres plus brutales telles que les droits de douane, les gels d'avoirs ou les embargos.

Enfin, un champ d'application en expansion de la compétition économique et de l'arme de l'ingérence concerne la normalisation.

A ces différentes menaces sont associés des risques qu'il convient d'anticiper. Au vu de leur possible impact sur la santé économique globale du pays et le niveau de l'emploi[142], on retiendra quatre risques majeurs. Tout d'abord, la perte de contrôle de fleurons industriels et technologiques dans des filières stratégiques et d'avenir. Les méthodes employées pour prendre le contrôle de ces entreprises « stratégiques » sont typiquement la captation des données, l'offre publique d'achat (OPA) hostile, le rachat ou la prise de participation agressive, des mesures de déni d'accès (par exemple le blocage de

---

[138] Information non attribuable

[139] Bank of America, *The threat mis- and disinformation pose to business*, 20 décembre 2023, « *The risks of mis/disinformation to organizations are threefold: reputational loss, financial loss and disruption of business objectives* ».

[140] Ministère des Armées, *Décryptage - La désinformation au service de la compétition industrielle ?* https://www.defense.gouv.fr/desinformation/nos-analyses-froid/decryptage-desinformation-au-service-competition-industrielle, consulté le 9 décembre 2025.

[141] Alice Vitard, « Naval Group dénonce une tentative de déstabilisation après la revendication d'une cyberattaque », *L'Usine Digitale*, 28 juillet 2025.

[142] Mathieu Duchâtel, Institut Montaigne, *op. cit.*

l'exportation de matériaux critiques) ou encore une politique d'attractivité (conditions de financement) pour faire venir aux États-Unis des filiales rendues ensuite « transparentes » et vulnérables. Ensuite, le risque d'une « fuite des cerveaux » qui s'intensifierait et de l'érosion du potentiel d'innovation qui en résulterait. En outre, nous paraît préoccupante la création de vulnérabilités politiques et économiques, par l'accumulation de pertes de souveraineté, donc la relégation en « seconde zone » par effondrement de sa crédibilité et de son influence sur la scène internationale. Enfin, à plus long terme, une forme d'inféodation cognitive et d'atteinte à sa propre matrice culturelle est à redouter.

Le cas Exaion

Ce cas récent où l'on parle confusément de souveraineté, de sécurité et d'ingérence économiques est emblématique des dilemmes qui se posent à la France en matière de stratégie économique, et est en ce sens illustratif du constat posé par la directrice de la DGSI et ses services, à savoir la difficulté à trouver le juste équilibre entre attractivité et souveraineté. En effet, un accord de cession publié le 11 août 2025, validé par l'État, prévoyait la vente pour 168 millions de dollars (144 millions d'euros) de la start-up Exaion, filiale à 100 % d'EDF, à la société américaine de minage de bitcoin Mara Holdings. D'ici 2027, via notamment une clause de non-concurrence, Mara Holdings prévoyait de passer à 75 % du capital d'Exaion contre 127 millions de dollars (109 millions d'euros) d'investissements supplémentaires[143]. Subitement, le gouvernement français a fait marche arrière et vient d'annoncer qu'il appliquerait le dispositif de contrôle des IEF, un instrument que les autorités françaises se targuent par ailleurs d'avoir récemment redynamisé[144]. De nombreux experts estiment en effet qu'Exaion, filiale issue d'EDF Pulse, « opère des services numériques responsables, des calculs haute performance, et des nœuds Web3 sur plusieurs réseaux », ce qui en fait « une brique d'infrastructure singulière »[145] que l'on ne saurait décorréler en outre de la démarche dite de « cloud de confiance » de type SecNumCloud destinée à faire face aux géants américains. On se trouve donc là au cœur des tensions et dilemmes posés par la compétition économique : Exaion est en difficulté financière, donc vulnérable, mais elle est aussi un instrument de souveraineté dans des domaines sensibles. Comment, dans ce contexte, « concilier ouverture capitalistique et maîtrise juridique des données » ?[146] À ce jour, trois scénarios types semblent envisageables :

- Une procédure IEF qui valide la vente mais l'encadre et impose des restrictions et clauses de « sauvegarde » ;

- Le rejet de l'offre américaine au profit d'une offre française, ce qui requiert la mobilisation de fonds souverains ;

- La « reconfiguration de l'actif » qui permettrait de concilier prise de participation étrangère et préservation des intérêts de souveraineté[147].

Ainsi, selon la clé de lecture que l'on adopte, les uns évoqueront dans ce cas précis le jeu normal de la compétition économique à gérer par des « compromis », tandis que les autres y verront un ciblage

[143] Esther Attias et Juliette Raynal, « Vente d'Exaion (EDF) : Bercy déchiré entre souveraineté et attractivité des start-up françaises », *La Tribune*, 26 août 2025.
[144] SISSE, entretien du 10 septembre 2025.
[145] Baptiste Leclercq, « Exaion : vente sous contrôle, promesse de « protection » et bataille pour la souveraineté », *ActuFinance*, 5 novembre 2025.
[146] *Ibid.*
[147] *Ibid.*

sous forme d'ingérence capitalistique portant atteinte aux intérêts supérieurs de la nation. Quoi qu'il en soit, la responsabilité de la France, au travers d'EDF, demeure : quel est notre objectif stratégique dans le domaine concerné et quels moyens, notamment financiers, sommes-nous prêts à y consacrer ?

Partie 2 - La prise en compte de la menace par la France : analyse critique des dispositifs existants et des actions menées

21 - Une prise de conscience tardive

On ne retracera pas ici l'historique précis des processus intellectuels, administratifs et opérationnels qui ont amené la France à se préoccuper des questions d'ingérence économique. On soulignera toutefois que notre pays eut l'occasion de sortir de sa léthargie pour faire face à ce phénomène dès 1994, à l'occasion de la publication d'un document fondateur, le « rapport Martre »[148]. Dès cette époque, la menace était identifiée et analysée, les enjeux évalués et des recommandations effectuées pour mobiliser l'équipe France jugée, déjà, en retard par rapport à ses « partenaires-concurrents ». S'ensuivirent des années que nous osons qualifier de coupable dilettantisme ou d'attentisme collectif, pourtant jalonnées par des publications phares telles que le « rapport Carayon » de 2003, mais aussi marquées par des affaires retentissantes et particulièrement dommageables (parmi lesquelles l'emblématique cas d'Alstom Power sous l'administration Obama), sans toutefois que le pouvoir politique se saisisse du dossier pour enclencher une dynamique collective en la matière[149].

Une délégation interministérielle à l'intelligence économique (D2IE), rattachée à Matignon, avait toutefois été créée en 2009, à la suite des conclusions des travaux précédemment cités auxquels on peut ajouter ceux du MEDEF sur l'IE en 2004, ou encore ceux d'Alain Juillet, Haut responsable chargé de l'intelligence économique (HRIE) au SGDSN de 2003 à 2009. La D2IE et le SCIE de Bercy (Service ministériel de coordination à l'intelligence économique) furent fusionnés en 2016 pour devenir le service du SISSE, placé sous l'autorité du Commissaire à l'ISSE, rattaché à la Direction Générale des Entreprises (DGE) de Bercy[150].

Il faut se rendre à l'évidence : il aura donc fallu attendre 2019 pour que soit décidée la mise en place d'une politique publique de sécurité économique, par la publication du décret 2019-206 du 20 mars[151]. Le réveil a sonné, ce qui en soi est encourageant. A tout le moins, cela témoigne d'une prise de conscience par l'État de l'urgence et de la gravité de la situation. Un certain nombre d'instruments ont depuis été mis en place (voir Partie 2, 22), dont on peut légitimement penser qu'ils contribueront à

[148] Travaux du groupe présidé par Henri Martre, *Intelligence économique et stratégie des entreprises*, Commissariat général du plan, février 1994, https://www.vie-publique.fr/files/rapport/pdf/074000410.pdf, consulté le 2 juillet 2025.

[149] Dans le cadre d'un entretien confidentiel, un expert des questions d'intelligence économique nous a confié que sa proposition, faite au Secrétaire général de l'Élysée sous le mandat Hollande, de mise sur pied d'une structure d'intelligence économique réorganisée et renforcée avait été accueillie avec un mélange déstabilisant d'ignorance et de détachement.

[150] Décret n° 2016-66 du 29 janvier 2016 instituant un commissaire à l'information stratégique et à la sécurité économiques et portant création d'un service à compétence nationale dénommé « service de l'information stratégique et de la sécurité économique, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031940456, consulté le 25 août 2025.

[151] Décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000038252109, consulté le 25 août 2025.

renforcer l'équipe France dans le combat à mener. Cependant, le Sénat, par le biais du rapport Lienemann-Lemoyne sur l'intelligence économique[152], dressait en 2023, vingt ans après le rapport Carayon, un constat préoccupant : il y est affirmé, données à l'appui, que la plupart des observations et avertissements formulés par les rapports successifs mentionnés supra demeurent en grande partie valables. L'équipe France se mobilise certes davantage, mais à quel effet ?

22 - La mobilisation des acteurs : une réalité, des progrès

Il ne s'agit pas ici d'établir un catalogue exhaustif des acteurs de la sécurité, du renseignement ou de la contre-ingérence économiques, ou de leurs capacités, mais plutôt d'apporter un éclairage sur les principaux constituants de l'architecture d'ensemble et sur certaines compétences, ou limitations, dont on peut tirer des enseignements utiles.

Le rôle de l'État : une mobilisation déterminée

Organisation centrale

Soulignons d'emblée que, de l'avis de tous les intervenants rencontrés, le rôle de la présidence de la République est déterminant et innerve l'ensemble du système, notamment sur le plan du renseignement, via la CNRLT en particulier, et les actions secrètes de la DGSE.

L'Élysée et la communauté du renseignement : une volonté d'agir, une réorganisation en conséquence

La loi du 24 juillet 2015 relative au renseignement[153] introduit le concept de sécurité nationale, à laquelle on devrait rattacher, comme le préconise M. Hayez, celui de sécurité économique[154], à l'instar de ce que font nos principaux concurrents.

Notons également qu'en 2019, au moment où est publié le décret, la communauté du renseignement rend publique sa stratégie nationale du renseignement (SNR)[155]. Dans celle-ci est explicitement assumé, pour la première fois, le rôle des services en matière économique, sur les plans défensif et offensif. En 2025, une nouvelle SNR est publiée, dans laquelle est mis en valeur le rôle des services en matière de souveraineté économique face à une « compétition économique débridée »[156], un constat qui n'a toutefois rien d'original.

[152] *Op. cit.*
[153] Loi n° 2015-912 du 24 juillet 2015 relative au renseignement, JORF n°0171 du 26 juillet 2015, consulté le 25 juillet 2025.
[154] Philippe Hayez, « Les entreprises françaises face aux services de renseignement étrangers », Paris, *op. cit.*
[155] CNRLT, *Stratégie nationale du renseignement*, janvier 2025, https://www.elysee.fr/admin/upload/default/0001/17/43c8a9bc0eef153b6041e6e68973bd7ac8c4c14e.pdf, consulté le 22 juillet 2025.
[156] *Ibid*., p. 9.

Des services qui œuvrent à la souveraineté économique

Les services de renseignement contribuent à la souveraineté économique de la France en concourant à la détection et à la neutralisation des menaces susceptibles de porter atteinte à nos intérêts économiques, financiers, industriels et scientifiques.

Inscrivant leur action dans le cadre du Plan « France 2030 », plan d'investissement de 54 milliards d'euros annoncé en 2021 par le président de la République, ils protègent au quotidien nos actifs stratégiques, entreprises et laboratoires notamment, dans un environnement concurrentiel exacerbé. L'appui à la promotion de notre économie constitue le deuxième volet de l'action des services dans le domaine du renseignement économique. Enfin, les services de renseignement participent à la lutte contre les fraudes aux finances publiques.

Source : CNRLT, SNR 2025.

Depuis, les services se sont réorganisés et dotés de structures et de moyens qui leur permettent effectivement de replacer la dimension économique au cœur de leurs priorités après deux décennies consacrées prioritairement à la lutte contre le terrorisme. À la faveur de moyens financiers en forte hausse depuis 2017, les services ont ainsi pu s'engager résolument en soutien de la politique publique.

La CNRLT : depuis 2017, elle dispose d'une vision d'ensemble et sert de courroie de transmission entre l'Élysée et les SR tout en jouant un rôle de conseil et d'orientation au sein de l'administration, entre services bien évidemment, mais aussi entre les services et quelques acteurs clés, en particulier le SGDSN. Elle s'appuie en outre sur le rapport Roux de Bézieux, dont les recommandations continuent d'irriguer l'écosystème national et d'alimenter les réflexions et actions : renforcement des liens entre les services de l'État et les entreprises, renforcement de la sensibilisation des entreprises à la sécurité économique, etc.

La DGSI : elle dispose d'une sous-direction de la protection économique, entièrement dédiée à ces problématiques, qui travaille au quotidien au sein de l'écosystème interministériel concerné (Élysée, Bercy, SGDSN, MINARM dont DRSD et DGA, etc.). Cette sous-direction travaille étroitement avec la DRSD, selon une logique désormais éprouvée de répartition des tâches, à partir de la même typologie des menaces par souci de cohérence, les dossiers étant partagés selon une délimitation assez nette entre ce qui ressortit à la BITD et ce qui concerne le reste des filières stratégiques non spécifiquement défense. Il y a néanmoins une zone « sensible » ou « grise » que les deux organismes s'efforcent d'appréhender avec le plus de justesse possible : il s'agit des biens à double usage. La DGSI, par l'entremise de cette sous-direction, a donc pour mission de protéger les actifs stratégiques, les actions de « promotion »[157] revenant à la DGSE exclusivement, mais aussi de développer ses capacités de détection et d'anticipation (analyse des tendances en matière d'évolution des menaces et identification des acteurs français pouvant à terme être ciblés). Elle constate que le modèle type des ingérences repose sur des stratégies articulant temps long (infiltration, actions de sape, etc.) et combinaison de différentes méthodes, en un tout parfois complexe à démêler et appréhender, et qu'en ce domaine les PME et ETI constituent le « ventre mou » de l'écosystème français. Enfin, en interne, la DGSI est consciente du besoin de disposer d'un niveau d'expertise économique élevé pour assurer sa crédibilité aux yeux des

[157] Il s'agit d'actions de soutien aux entreprises françaises, par divers moyens, afin de leur permettre d'accéder à des marchés porteurs par exemple.

entreprises; pour cela, elle cherche à diversifier les compétences en son sein, mais, contrairement à ce qui est habituel chez nos partenaires anglo-saxons, elle constate que le monde du renseignement et le monde de l'entreprise demeurent étrangers l'un à l'autre.

La DGSE : elle s'est également réorganisée autour de pôles de compétences ou centres de mission dont l'un est entièrement dédié aux questions économiques. Sa mission première est donc de promouvoir les intérêts français dans ce domaine, par différentes mesures, de nature proactive (entrave, soutien à l'implantation d'entreprises françaises par exemple) via l'identification et l'exploitation d'opportunités (vulnérabilités étrangères). Toutefois, la conduite, en soutien d'entreprises, d'actions véritablement offensives qui requièrent la mobilisation de capitaux n'est pas aussi développée qu'elle peut l'être aux Etats-Unis ou en Chine, faute de moyens suffisants.

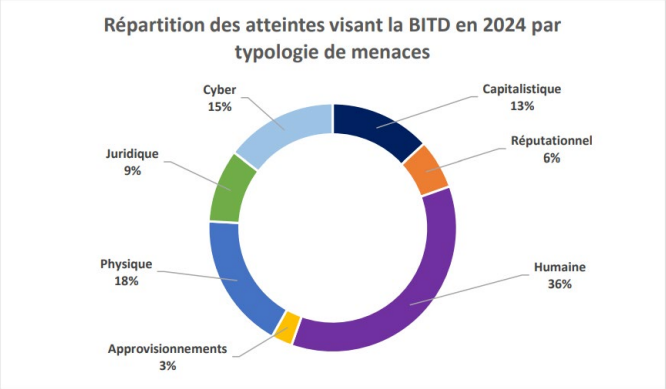
La DRSD : elle a pour mission première de protéger (contre-ingérence) la BITD constituée des entreprises opérant au profit de la défense nationale, mais aussi, et c'est aujourd'hui une priorité, des centres de recherche et des laboratoires qui en sont de fait la matrice. Les menaces sont analysées selon le « prisme TESSCo – terrorisme, espionnage, sabotage, subversion, crime organisé ». Un effort particulier porte sur le contrôle par la France de ses chaînes d'approvisionnement et de valeur, et sur la maîtrise de l'écosystème constitué par les ETI-PME-TPE et l'ensemble des sous-traitants. Selon la DRSD, les tensions augmentant, les ingérences économiques se multiplient et se diversifient, facteur aggravé par le fait que sous l'impulsion du rythme frénétique de la « révolution technologique » en cours, l'écosystème international est extrêmement dynamique et changeant, ce qui complexifie son suivi[158]. Ainsi, le véritable défi consiste désormais à protéger le savoir par la rapidité d'innovation, ce qui place donc l'information, c'est-à-dire la donnée, au cœur de toute stratégie : obtenir la donnée à temps et la traiter avant obsolescence implique une coopération très étroite entre services, entre la DRSD et les milieux universitaires et centres de recherche, et l'utilisation d'outils numériques de traitement à la pointe de la technologie[159]. Ces menaces peuvent représenter une atteinte à la souveraineté nationale dans des domaines extrêmement sensibles, mais aussi, ne l'oublions pas, peuvent avoir un effet d'érosion de l'aptitude opérationnelle des forces si les mesures de protection faillissent, le cas le plus conséquentiel pouvant concerner la force de dissuasion nucléaire. La DRSD coopère donc étroitement avec le ministère de l'enseignement supérieur et de la recherche (MESR), les institutions académiques et l'ensemble de la « communauté de la recherche », en partenariat, au sein du MINARM, avec la DGA et l'Agence de l'innovation de défense. Elle a mis en place et anime un dispositif de sensibilisation auprès des entreprises concernées constitué d'interventions humaines, de conférences, mais aussi de guides pratiques. Récemment, la DRSD, en partenariat avec le Cercle des directions de la Sécurité des entreprises (CDSE), a publié un outil-guide méthodologique destiné à faciliter la conception et la mise en œuvre d'un plan de continuité d'activité (PCA) au sein des TPE et PME[160]. Cette initiative vient compléter la parution en 2023 du « guide pratique d'analyse de

[158] Général Bonnemaison, « Anticiper les menaces pour protéger notre souveraineté nationale », *Esprit Défense* N° 17, automne 2025, https://www.defense.gouv.fr/sites/default/files/drsd/Esprit%20d%C3%A9fense%20n%C2%B0%2017%20-%20Automne%202025.pdf, consulté le 24 novembre 2025.

[159] *Ibid*. Citons l'exemple du Système d'information du renseignement de contre-ingérence de la défense (Sircid), un outil d'analyse fondé sur l'intelligence artificielle et les mégadonnées (*big data*), Sircid permettra de corréler des données apparemment sans lien, comme des personnes ayant fréquenté les mêmes lieux.

[160] DRSD, *Méthode flash du guide* : https://www.defense.gouv.fr/sites/default/files/drsd/Elaboration%20PCA%20m%C3%A9thode%20Flash.pdf

risques »[161] et, en 2024, du « guide de survie face à la crise »[162]. Enfin, en lien avec la DGSI[163], elle vient de publier un document à l'attention des entreprises en les sensibilisant à la protection de leurs droits de propriété intellectuelle, cibles des ingérences étrangères[164].



Source : DRSD, Lettre d'information économique, « *Panorama des ingérences à l'encontre de la sphère de Défense en 2024* », juillet 2025

La DNRED : elle fait désormais de la « défense économique » un objectif prioritaire et poursuit un effort de restructuration interne, en administration centrale et sur le terrain : renforcement des compétences en la matière au sein du département contre-prolifération et sanctions ; dispositif de référents « sécurité économique » au sein du réseau douanier de chaque région ou encore réorganisation du fonctionnement du réseau des attachés douaniers. Dans sa mission de renseignement économique, la DNRED coopère étroitement avec le SISSE tandis que sur le plan de la sécurité économique, elle œuvre en collaboration avec l'ensemble des entités de Bercy concernées (DGT par exemple). Les douanes sont confrontées à des acteurs redoutables, en particulier la Chine, laquelle se distingue par sa maîtrise de la chaîne logistico-commerciale, du producteur jusqu'au consommateur. Son « *business model* » est fondé sur la défiscalisation et recourt à une organisation logistique opaque incluant la participation de la diaspora (stockage des marchandises, gestion locale), la remontée des flux financiers (blanchiment) jusqu'en Chine par des relais en Europe (sociétés), ou encore l'exploitation des plateformes (ports et aéroports) qui servent à contourner les dispositifs de contrôle et de taxation[165]. Autre acteur problématique, les Etats-Unis recourent à plusieurs outils que sont les finances, le *lawfare* et la technologie pour contourner des règlements français ou européens et entretenir des mécanismes financiers suspects (défiscalisation au Delaware, un État fédéré qui peut être considéré comme un paradis fiscal[166]).

[161] DRSD, septembre 2023, https://www.defense.gouv.fr/sites/default/files/drsd/20230921-Guide-pratique-analyse-de-risques-DRSD-DPID.pdf, consulté le 24 novembre 2025.

[162] DRSD, décembre 2024, https://www.defense.gouv.fr/sites/default/files/drsd/GUIDE%20SURVIE%20CRISE-DRSD-BLN.pdf, consulté le 24 novembre 2025.

[163] DGSI, *Flash ingérence N°7 / Octobre 2025 : Risques associés à l'absence de protection des logiciels à usage industriel*, https://www.dgsi.interieur.gouv.fr/dgsi-a-vos-cotes/contre-espionnage/conseils-aux-entreprises-flash-ingerence, consulté le 24 novembre 2025.

[164] DRSD, « La propriété intellectuelle au sein de la sphère de défense », *Lettre d'Information Économique* N° 21 / Octobre 2025, https://www.defense.gouv.fr/sites/default/files/drsd/LIE%20n%C2%B021%20-%20Propri%C3%A9t%C3%A9%20intellectuelle%20dans%20la%20sph%C3%A8re%20d%C3%A9fense.pdf, consulté le 24 novembre 2025.

[165] Des informations complémentaires, non attribuables, obtenues auprès d'autres responsables de l'administration ou experts révèlent que la Chine se livre systématiquement à des tentatives de corruption des acteurs du contrôle, ce qu'elle est parvenue à faire avec efficacité dans le temps en Tchéquie et en Hongrie par ex.

[166] Environ 50% des sociétés américaines cotées en bourse à New York ont leur siège social au Delaware.

La DNRED souligne l'importance de la coopération intra-européenne, les progrès accomplis et réformes en cours[166], mais déplore les divergences nationales et l'absence de « culture douanière » chez nombre de pays européens.

Le Décret de 2019 et le rôle central de Bercy : une lourde responsabilité à assumer

Le décret n° 2019-206 du 20 mars 2019 relatif à la gouvernance de la politique de sécurité économique qui fonde la politique publique en la matière, assigne comme mission principale d'« assurer la défense et la promotion des intérêts économiques, industriels et scientifiques de la Nation, constitués notamment des actifs matériels et immatériels stratégiques pour l'économie française », et « inclut la défense de la souveraineté numérique ». Un rôle central est ainsi confié au Comité de liaison en matière de sécurité économique (COLISE), présidé par le SGDSN et regroupant la CNRLT ainsi que tous les ministères concernés, qui a en charge « l'instruction des décisions proposées au conseil de défense et de sécurité nationale en matière de sécurité économique et le suivi de leur mise en œuvre »[167]. En son article II, il confie un rôle prépondérant au CISSE[168] et donc au MINEFI, et à son bras armé, le SISSE, où est censée se concevoir la politique de sécurité économique nationale.

Le SISSE assure donc la gouvernance de la politique de sécurité économique sous l'autorité du Conseil de défense et de sécurité nationale (CDSN) et du COLISE. Il conçoit sa mission première comme étant d'assurer la protection des actifs stratégiques français, donc selon une approche exclusivement défensive. Dans le cadre de la consultation interministérielle, il valide la liste des secteurs stratégiques et est ainsi en mesure d'orienter les différents acteurs nationaux. Sa compétence désormais reconnue, y compris à l'étranger, le SISSE se déploie dans les régions (voir p. 46) où il mène, via les DISSE, de nombreuses actions de prévention et d'information (diffusion d'outils d'auto-diagnostic, 28 fiches réflexes, etc.). Il conduit également une action d'influence auprès des autorités de l'UE (voir p. 56).

Partant du constat de l'ampleur des menaces (1000 alertes par an dont 300 aboutissent à l'établissement d'un dossier), de leur nature (diversifiée mais majoritairement capitalistique) et de leur origine (Etats-Unis en premier rang, Chine en phase de montée en puissance, puis les partenaires européens en particulier), le SISSE estime, d'une part, que des progrès indéniables ont été réalisés sur le plan national via notamment l'élaboration d'un référentiel d'investissement, l'adaptation des procédures administratives, et une meilleure circulation de l'information entre administrations, et, d'autre part, pointe l'importance croissante de l'outil qu'est le contrôle des investissements étrangers en France (CIEF). Or, cet instrument, placé pour des raisons historiques au sein de la DGT, n'a pas été conçu comme un outil de politique industrielle mais d'ordre public et de défense nationale, donc dans un esprit très défensif et une pratique restrictive[169]. Le CIEF est désormais davantage utilisé, mais encore perfectible malgré les efforts accomplis, en particulier dans sa dimension du contrôle aval[170]. Les autorisations d'investissement accordées à des partenaires ou concurrents étrangers après lancement d'une procédure de CIEF (environ 100 lettres d'engagement par an) stipulent des conditions d'exécution telles qu'une séparation des réseaux cyber internes, la constitution d'une unité juridique française ou l'établissement d'un siège d'entreprise en France, etc. qui doivent, pour que l'édifice soit crédible – et éventuellement dissuasif – être contrôlées efficacement, dans la durée. Or, dans les faits, la France a encore beaucoup à apprendre de ses retours d'expérience pour exercer

[166] Une réforme de l'Union douanière a été lancée le 17 mai 2023 par les instances européennes, avec la mise en place de l'Alliance douanière européenne pour les frontières (ADEF) en 2025, qui préfigure la future Autorité.

[167] *Décret n° 2019-206*, op. cit.

[168] *Ibid.*

[169] Décret n° 2023-1293 du 28 décembre 2023 relatif aux investissements étrangers en France, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000048706234, consulté le 19 septembre 2025.

[170] Le SISSE confirme qu'en moyenne 100 à 120 contrôles du respect des conditions par les investisseurs sont effectués chaque année. Les enseignements tirés sont présentés à la Direction générale du Trésor ainsi qu'au Comité interministériel des investissements étrangers en France (CIIEF).

un contrôle aval performant, d'autant que la mainmise de Bercy sur le CIEF, y compris dans sa dimension contrôle aval, ne convainc pas toutes les administrations qui semblent privilégier un transfert au niveau interministériel. Enfin, et c'est là l'essentiel, le SISSE considère que la bataille se joue principalement autour des capitaux, ce qui place en première ligne la DGT et non pas le SISSE. Le financement des entreprises françaises, en particulier des start-ups prometteuses, est un défi quotidien : mobiliser les finances publiques et privées (action de la Banque publique d'investissement (BPI) ou de l'Agence des participations de l'État (APE) par exemple), et attirer des capitaux « alliés », au profit des filières stratégiques, constitue une priorité absolue. Et c'est aussi dans ce domaine que s'exerce la plus vive concurrence.

La coordination gouvernementale et les services du Premier Ministre

Le SGDSN-COLISE-PPST : un effort de cadrage et de coordination à des fins de cohérence et d'efficacité

Le SGDSN a de longue date joué un rôle éminent en matière de « sécurité économique » puisqu'il a notamment hébergé la fonction « intelligence économique » de 2003 à 2009, pilotée à l'époque par M. Alain Juillet. Aujourd'hui, il agit principalement selon deux axes : d'une part, l'expertise en matière de protection du patrimoine scientifique et technologique (PPST) ; d'autre part, sa mission de cadrage, coordination (dont présidence du COLISE) et « conseil » (recommandations à l'attention du PM) dans plusieurs domaines dont le cyber (en lien avec l'ANSSI et le Centre de coordination des crises cyber-C4) et le contrôle des exportations, une mission historique à vocation première de contre-prolifération qui doit aujourd'hui prendre en compte un contexte international et des pratiques, notamment sous influence américaine, qui transforment cette mission régalienne en instrument de « guerre économique ».

Par ses activités, le SGDSN bénéficie d'une vision à la fois globale et précise de la menace, des enjeux et des défis associés. Son analyse de la menace fait ressortir qu'historiquement, Etats-Unis et Royaume-Uni, et plus récemment, Allemagne, Corée du Sud ou encore Israël sont des acteurs très impliqués et parfois très agressifs à l'encontre de la France. Ils ont été rejoints par la Chine, désormais en volume et en intensité le pendant des Etats-Unis. Les principaux outils d'ingérence à l'échelle nationale sont tout d'abord la montée au capital, qui peut aujourd'hui être mieux contrée par l'application du filtre du CIEF. En matière de capital, un nouvel enjeu de taille concerne toutefois le contrôle des capitaux sortants (de type *Reverse-CFIUS* aux Etats-Unis). On notera enfin une faiblesse du dispositif CIEF qui ne couvre pas, en vertu des dispositions de l'article R. 151-2 du code monétaire et financier, les investissements « *greenfield* » (investissements directs à l'étranger), ce qui peut créer une distorsion de concurrence à terme[170]. Est également souligné l'usage du droit, notamment dans le cadre du contrôle des exportations de biens à double usage où les mesures américaines et chinoises durcissent de plus en plus les règles du jeu et équivalent parfois à des mesures coercitives (cas de la politique chinoise des terres rares et minerais critiques pensée pour obtenir un droit de regard sur les capacités et projets d'entreprises concurrentes, ou encore de mesures prises par les Etats-Unis pour empêcher l'UE d'exporter certains biens vers la Chine). Cet arsenal se déploie historiquement par différents canaux (cabinets de conseil et de conformité) dont les États-Unis sont les pionniers. La Chine commence à déployer des capacités en miroir tandis que la filière française brille par son absence. Enfin, sont relevées les activités de captation-prédation. Les techniques utilisées sont nombreuses et bien identifiées, qu'il s'agisse de la cybermenace, du débauchage (de cadres, de « têtes grises » dans les universités et laboratoires de recherche) ou de l'infraction. Sur le plan juridique, la France doit faire face à plusieurs lacunes de ses dispositifs. De manière symptomatique, elle ne dispose pas d'outil juridique lui permettant de s'opposer au débauchage d'un chercheur retraité ou de responsables civils

[170] Ministère de l'économie, des finances et de la souveraineté industrielle et numérique, Direction Générale du Trésor, Lignes directrices relatives au contrôle des investissements étrangers en France, 2024, p. 12.

de haut niveau dans des grands groupes, l'article 42 de la LPM couvrant le seul domaine militaire (BITD)[171].

Le SGDSN œuvre en outre à la protection du patrimoine scientifique et technologique (PPST) et est pour cela en contact étroit avec tous les acteurs publics et privés concernés, notamment les universités, laboratoires ou centres de recherche. En 2024, face à une menace qui ne faiblit pas, un nouveau régime contraventionnel a été mis en place, qui confère ainsi plus de poids à l'autorité publique lors des discussions engagées avec les laboratoires de recherche en particulier, auquel est attaché un principe de conditionnalité des aides publiques. Concrètement, pour qu'un laboratoire travaillant dans des domaines sensibles puisse bénéficier de fonds publics, il devra satisfaire à certaines obligations en matière de sécurité et de protection (établissement d'une Zone à régime restrictif-ZRR, protection de la propriété intellectuelle, etc.). L'administration, dans un effort parfaitement légitime et aujourd'hui impérieux de conviction – car ces mesures ne sont pas toutes légalement obligatoires - dispose donc désormais de mesures plus contraignantes et de leviers contractuels dans son action. Des progrès sont donc constatés, mais les déficiences culturelles ne sont pas pour autant résorbées : le retard français dans ce domaine demeure[172].

Ainsi, si l'arsenal français s'étoffe, le constat est fait d'une utilisation très limitée des outils à disposition. En matière de travaux pratiques, la loi Sapin II n'a pas été activée (article 40), de même que la « loi de blocage » de 1968 n'a jamais été mise en œuvre dans des cas majeurs[173]. Toutefois, le mécanisme CIEF est en place et actionné au besoin, tandis que des mesures d'entrave, par définition confidentielles, sont prises régulièrement. On notera par ailleurs que la base juridique française soutenant cet arsenal n'est pas jugée solide par certains acteurs, et que pour aller plus loin dans les dispositifs contraignants, il faudrait procéder à une réforme du Code de travail, un chantier à ce jour hors de portée[174].

Un autre atout théorique dans la manche de l'administration est la capacité d'action de l'UE qui s'est dotée, comme on l'a vu, de dispositifs de « protection » dans le cadre d'une stratégie de sécurité économique. Là encore, il faut bien distinguer les intentions et outils de leur application effective. L'expérience montre que la situation est plus complexe qu'il y paraît (voir *La pertinence de notre organisation : peut-on parler d'une « équipe France » ?* p. 56).

Enfin, plus largement, le SGDSN souligne qu'il convient de trouver un équilibre entre des actions défensives et des actions offensives car une focalisation excessive sur les premières peut avoir pour effet de détourner des investissements étrangers utiles ou de limiter les investissements européens à l'étranger.

Le ministère des Armées (MINARM), ses services et la DGA : un ensemble robuste au défi de la diversification et de l'intensification des menaces

Le MINARM a sous son autorité trois services de renseignement dont deux, la DGSE et la DRSD, jouent un rôle majeur en matière de lutte contre les ingérences économiques. Un autre acteur occupe une

[171] Loi n° 2023-703 du 1er août 2023 relative à la programmation militaire pour les années 2024 à 2030 et portant diverses dispositions intéressant la défense (1), Titre II : Dispositions normatives intéressant la défense nationale (Articles 13 à 71), Chapitre II : Renseignement et contre-ingérence (Articles 40 à 46), JORF n°0177 du 2 août 2023, consulté le 25 novembre 2025 .

[172] D'échanges avec des étudiants ou employés au sein d'écoles et d'universités, l'École nationale de l'aviation civile (ENAC) et l'université de la Rochelle notamment, il ressort que les contrôles en ZRR demeurent parfois très permissifs. Une base de données de l'ENAC permettant d'établir la cartographie des chercheurs et des thèmes étudiés est ainsi accessible (et exploitée par les ressortissants de nationalité chinoise en particulier).

[173] Sur ce point, le SISSE précise que depuis la réforme de 2022, 50 à 75 avis par an ont été formulés par ses soins et produits devant les juridictions compétentes, et ont parfois concerné des entreprises stratégiques.

[174] SGDSN, entretien du 8 septembre 2025.

place centrale dans le dispositif national, au profit de la BITD : il s'agit de la DGA, qui a mis sur pied le 23 février 2024 une direction de l'industrie de défense (DID)[174] dont le service de la sécurité économique (SSE) agit selon deux axes : l'un de protection économique, l'autre d'intelligence économique.

La sous-direction de la Protection et de la Résilience des Entreprises focalise ses efforts sur trois domaines. Premièrement, le contrôle des IEF dont elle instruit environ 50% des dossiers pour avis. Dans ce domaine, par-delà la motivation des refus ou l'acceptation sous conditions, l'enjeu véritable consiste à attirer des capitaux français. Ce travail est effectué en coordination avec Bercy et pourrait être facilité à terme par le recul du carcan des régulations européennes qui venaient contraindre l'écosystème défense[175]. La commande publique, qui augmente, joue évidemment un rôle déterminant, mais elle doit s'accompagner d'investissements privés que le Club des investisseurs de la défense, entre autres, s'efforce de mobiliser[176]. Deuxièmement, le contrôle de la propriété intellectuelle par le suivi des « mises au secret » faites par les entreprises, en coordination avec l'Institut national de la propriété intellectuelle (INPI) pour la sensibilisation des entreprises, en particulier les PME. Enfin, la mise en place en juin 2024 d'un référentiel de sûreté et de maturité cyber dit CCIA (Conseil pour la Cybersécurité de l'Industrie d'Armement), en coordination avec l'ANSSI, la DRSD (via le Computer Emergency Response Team-Entreprises de Défense-CERT[ED])[177] et l'industrie, en un effort constant d'adaptation à un milieu très dynamique.

La sous-direction multiplie les déplacements sur sites (900 visites par an) afin d'accompagner les entreprises (sur les 4500 entreprises, 1000 sont considérées « critiques »). D'autre part, elle cherche à développer ses capacités d'anticipation et à prévenir certains risques, en particulier cyber, liés à la propriété intellectuelle ou encore aux normes, spécifiquement l'ITAR américain qui continue de représenter un défi considérable au vu de l'imbrication des BITD française et américaine, ou encore la réglementation de conformité que de nombreuses banques et entreprises redoutent.

Le cas Nawa Technologies

La problématique ITAR est connue de longue date, au point que nous parlons désormais d'un objectif de « désitarisation » rendu nécessaire par les trop fortes contraintes exercées sur l'écosystème de défense français par les règlements américains. Malgré nos efforts, certains de nos acteurs restent fragiles, en particulier les PME et start-ups. Tel est le cas de la pépite Nawa Technologies, une « *deeptech* » spécialisée dans les matériaux innovants (nanotubes de carbone), qui cherche à pénétrer le marché américain et à s'installer en Floride, à Dayton, pour travailler avec l'US Army notamment. La start-up est certes accompagnée par la DGA, mais en interne, les compétences lui font défaut. En effet, maîtriser la configuration labyrinthique de l'ITAR requiert des moyens et des qualifications que ne peut posséder une jeune société. Dès lors, selon l'aveu même de personnes en charge du dossier au sein de l'entreprise, le besoin est celui non pas d'un simple accompagnement, mais d'une prise en main et

[174] La DGA s'appuie en outre sur des attachés de l'industrie de défense en région (AIDeR) qui sont en contact avec l'écosystème territorial (CIC, Conseil régional, agences territoriales de développement, pôles de compétitivité, etc.).
[175] Certaines banques disposent désormais de référents défense.
[176] Lancé par le DGA le 22 juin 2025.
[177] Ministère des Armées, *Description CERT [ED] Computer Emergency Response Team Entreprises de Défense RFC 2350*, DRSD, https://www.defense.gouv.fr/sites/default/files/drsd/CERT-ED_RFC_2350.pdf, consulté le 3 décembre 2025.

d'une formation véritable dans la durée par la DGA ou tout autre acteur compétent. On se heurte alors à la disponibilité des moyens des uns et des autres. Tel est le constat de la réalité opérationnelle à laquelle se confronte une jeune société innovante non configurée pour faire face à de tels impératifs bureaucratiques et réglementaires.

La sous-direction Intelligence économique (SDIE) conduit des missions d'investigation à partir de sources ouvertes, d'influence et d'intelligence offensive, c'est-à-dire d'appui à la conquête de marchés et de prise de contrôle éventuelle de fournisseurs étrangers constituant des maillons clés de la chaîne d'approvisionnement. LA SDIE est unique en ce sens qu'elle est la seule structure véritablement dédiée à l'offensive qui agisse au profit de la BITD, indépendamment évidemment des actions menées par la DGSE. Une nouvelle initiative a récemment vu le jour, les Rencontres de l'Intelligence Économique de Défense (RIED), organisée en cinq commissions, dont les résultats des travaux sont attendus pour le printemps 2026[178]. Il s'agit avant tout de fédérer l'écosystème et de coordonner les actions menées par différents organismes (État, industrie, monde académique, acteurs privés) afin d'augmenter l'efficacité des actions conduites.

Les préfets et les échelons déconcentrés : un rôle éminent reconnu mais encore fragile dans les faits

Toutes les études effectuées ces dernières années et déjà citées en référence dans celle-ci montrent combien l'échelon territorial est devenu un enjeu prioritaire au fil du temps, après avoir été longtemps négligé par les autorités centrales. Or, nos adversaires ne s'y trompent pas et savent qu'une approche indirecte qui contourne les dispositifs de l'administration centrale française leur permettra d'identifier des opportunités et de créer des vulnérabilités dans les territoires.

C'est pourquoi l'administration, par la circulaire du 12 juin 2019 portant sur la réforme de l'organisation territoriale précise que : « L'intervention de l'État sera recentrée sur l'accompagnement des entreprises en difficulté, ainsi que sur le suivi des filières stratégiques, des politiques d'innovation et de transformation numérique. Ces missions seront exercées au sein d'un service économique de l'État en région toujours placé dans les DIRECCTE (désormais DREETS). Les compétences relatives au tourisme, à l'artisanat - sauf en Corse et dans les outre-mer - au développement économique des territoires, sont de la compétence des régions et l'État, qui n'exerce d'ores et déjà plus que des missions résiduelles en la matière, cessera d'intervenir dans ces domaines »[179]. Les attributions des préfets de région et de département en matière d'économie et de sécurité économique sont donc renforcées, et certains services sont déconcentrés avec affectation de représentants à certains étages du « millefeuille administratif ». Ces dernières années, plusieurs initiatives complémentaires sont venues densifier le dispositif territorial ; on citera, sans souci d'exhaustivité :

- 23 DISSE (délégués du SISSE) en région agissant en lien avec les Commissaires aux restructurations et à la Prévention des difficultés des entreprises (CRP) et les Directions régionales de l'Économie de l'Emploi et des Solidarités (DREETS), sous la coupe du Secrétaire Général pour les Affaires Régionales (SGAR) ;
- La systématisation des détachements d'équipes d'assistance (technique ou de conseil) de la part, à titre d'exemple, de la DGSI, de la DGA ou de la DRSD (environ 180 missions par an) ;

[178] DGA, Lancement des « Rencontres de l'intelligence économique de Défense (RIED) 2025 », 17 juillet 2025, https://www.defense.gouv.fr/dga/actualites/lancement-rencontres-lintelligence-economique-defense-ried-2025, consulté le 30 septembre 2025.

[179] JORF, Circulaire du 12 juin 2019 relative à la mise en œuvre de la réforme de l'organisation territoriale de l'État, 13 juin 2019, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000038599066, consulté le 20 octobre 2025.

- Le rôle du CERT-FR (*Computer Emergency Response Team*) au niveau national et des CSIRT territoriaux (*Computer Security Incident Response Team*) de l'ANSSI qui sont des centres de réponse aux incidents cyber au plus près des entités implantées sur leurs territoires ;
- Les directions zonales de la DGSI.

Le rôle du préfet délégué pour la défense et la sécurité (PDDS) : une vision du terrain particulièrement précieuse

Le décret du 18 mars 1993 régit la fonction des PDDS qui ont été mis en place au fil du temps selon les régions. Le PDDS *« assiste le préfet de zone pour toutes les missions concourant à la sécurité publique, à la sécurité civile et à la défense de caractère non militaire »*[180]. Dans ses fonctions, il agit en étroite collaboration avec les nombreux organismes territoriaux (services associés de l'État, gendarmerie, douanes, Attachés de sécurité intérieure-ASI, etc.) et les services de renseignement du 1er cercle.

L'étude du cas de la région Auvergne-Rhône-Alpes (AURA), deuxième région française sur le plan économique, dont le rayonnement est international, permet de mettre en valeur plusieurs actions telles que l'action préventive et d'anticipation du préfet de région (SGAR) qui conduit une politique d'investissement (50 Mds d'euros en 2024), l'existence d'une feuille de route régionale pour la sécurité économique (2025-2027) qui concerne 400 entreprises et 40 000 chercheurs, et contient un plan d'action décliné dans chaque département[181] et, enfin, la mise en œuvre d'un plan « résilience zonale AURA » qui fait effort sur la connaissance la plus fine possible des PME et des chaines d'approvisionnement[182]. Cette connaissance permet de détecter des IEF potentiellement problématiques qui sont remontés par la chaîne administrative, du SGAR à la DGT.

La structuration de son dispositif de protection économique mais aussi de détection et d'anticipation permet de constater une recrudescence des ingérences ou tentatives d'ingérence, et notamment l'intensification des actions conduites par les partenaires européens, en particulier l'Allemagne et l'Italie depuis trois ans. Malgré les progrès – et les efforts – indéniables effectués ces dernières années, la sécurité en général et la cybersécurité en particulier demeurent problématiques tant elles se heurtent à des déficiences persistantes au sein du réseau des ETI-PME et, plus généralement, à une psychologie collective encore trop indifférente aux risques. Les acteurs locaux estiment que, plus que jamais, la granularité des niveaux départemental et régional est essentielle à la bonne appréhension des menaces et à la juste application des mesures de contre-ingérence.

---

[180] JORF, Décret n°93-377 du 18 mars 1993 relatif aux préfets délégués pour la sécurité et la défense auprès des préfets de zone de défense, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000347247/, consulté le 20 octobre 2025.

[181] Préfète Fabienne Buccio, *L'État s'engage pour la sécurité économique des entreprises*, Préfecture AURA, Sécurité économique région AURA.pdf, consulté le 21 octobre 2025. Voir également le dispositif CIEF de la région AURA, Intel éco AURA synthèse 2024.pdf, consulté le 21 octobre 2025.

[182] Il s'agit de la déclinaison du Plan national de relance et de résilience (PNRR), https://www.prefectures-regions.gouv.fr/auvergne-rhone-alpes/Region-et-institutions/L-action-de-l-Etat/France-Relance-en-Auvergne-Rhone-Alpes/France-Relance-dans-vos-departements/France-Relance-dans-votre-departement, consulté le 21 octobre 2025.

Le rôle des entreprises : des acteurs au cœur de la mêlée, sensibilisés, mais soumis à forte contrainte

Le constat préoccupant et l'action déterminée du MEDEF

Le rapport Roux de Bézieux, du nom de son auteur, ancien président du MEDEF, témoigne du dynamisme et du volontarisme du Mouvement qui est parfaitement conscient des enjeux ainsi que des difficultés rencontrées au quotidien par les entreprises françaises de toute taille.

Au sein du MEDEF, la Commission « souveraineté et sécurité économiques des entreprises », mise en place en 2018, a permis de positionner le MEDEF dans l'écosystème national et de considérablement accroître le niveau d'interaction entre entreprises, administration, services de renseignement et autres acteurs, y compris dans les territoires (préfectures, gendarmerie, etc.) grâce à ses structures régionales.

Le constat du MEDEF est toutefois nuancé et souligne, indépendamment de la question des moyens financiers nécessaires pour protéger des entreprises stratégiques vulnérables ou partir à la conquête de marchés, les progrès qui restent à accomplir dans plusieurs domaines pour nous crédibiliser. En premier lieu, s'agissant de l'état de la menace et du périmètre d'action, le partage d'une information complète sur le nombre et la nature des actions étrangères, et sur l'état de nos dépendances et du risque économique, n'est pas assuré et ne permet pas aux entreprises d'avoir une juste représentation de la situation. La commission évoquée supra recommande la mise en place d'un observatoire qui produise des données et statistiques précises et concrètes afin de contribuer à la sensibilisation des entreprises aujourd'hui relativement indifférentes aux chiffres officiels communiqués qui rapportent 1000 alertes annuelles par an pour un écosystème composé de 8000 entreprises « stratégiques » sur 240000. Ce constat amène à une autre réflexion concernant le périmètre de la sécurité économique en France, aujourd'hui limité à la BITD et à un certain nombre d'entreprises opérant dans des filières stratégiques : faut-il s'en contenter ou faut-il élargir ce périmètre pour porter le défi à l'échelle nationale et impliquer véritablement l'ensemble des acteurs, comme l'affaire Shein pourrait le suggérer ? Un deuxième sujet de préoccupation concerne la fragilité des territoires et des PME : toucher les acteurs dans les régions françaises, ETI, PME et TPE, n'est pas chose aisée. Le « tour de France » de M. de Bézieux y a contribué, mais le chemin à parcourir demeure long et sinueux. L'organisation nationale reste assez peu connue de ces acteurs et trop complexe pour qu'ils puissent l'appréhender avec l'efficacité requise. Sur le plan territorial, elle est encore assez récente et fragile, et dépendante de l'implication personnelle des quelques individus en charge. Enfin, les opérations de sensibilisation et de formation existent, mais elles ne permettent pas encore d'infléchir la culture française en ce domaine[183]. Enfin, un défaut de vision et d'organisation de niveau stratégique est déploré. Pour le MEDEF, l'existence du Plan de relance 2030 et du Haut-Commissariat à la stratégie et au plan ne fait pas une stratégie. L'absence de directives partagées comme de priorités assumées, l'impossible identification de la structure de pilotage et la multiplicité des acteurs administratifs rendent l'écosystème peu lisible et sans doute moins efficace qu'escompté.

Le cas des grands groupes : des acteurs autonomes, avertis et résilients

Les grands groupes français sont à la fois sensibilisés à ces questions, par leurs opérations à l'échelle internationale, et suffisamment armés pour relever les défis qui se présentent à eux, non sans peine parfois puisqu'il s'agit bien d'un combat quotidien. Les organisations adoptées par ces groupes

[183] Le MEDEF souligne l'excellente initiative prise par l'ESTA de Belfort qui a mis en place un cycle de « souveraineté économique », et remarque par ailleurs que les programmes de géopolitique des grandes écoles comme HEC ou l'ESSEC demeurent trop génériques et devraient inclure une composante « sécurité économique » bien plus développée.

relèvent en grande partie du cœur de métier, des priorités opérationnelles et de la culture de l'entreprise concernée, ce qui explique que les dispositifs d'intelligence économique et de sûreté par exemple varient de l'une à l'autre.

Ainsi, les directeurs de sûreté-sécurité ou équivalents des grands groupes français du CAC 40 et du SBF 120, qui animent également la fonction « intelligence économique », sont regroupés au sein du Cercle des directions de la sécurité des entreprises (CDSE) et constituent une communauté active au sein de laquelle sont échangés expériences et pratiques[184].

Le milieu académique de la recherche et de l'intelligence économique : des compétences indéniables, un rayonnement insuffisant

Depuis les années 1990, de nombreux politiques et experts ont cherché à encourager le développement d'une école française de l'intelligence économique qui puisse essaimer dans les structures des milieux politico-administratif et de l'entreprise. Les rapports Martre et Carayon bien sûr, mais aussi plus récemment le rapport Lienemann-Lemoyne doivent beaucoup à la contribution d'experts, parmi lesquels MM. Harbulot, Moinet ou encore Juillet. On soulignera également les travaux novateurs de la Chaire renseignement de l'IEP d'Aix-en-Provence, en particulier ceux conduits sous la direction de M. Jean-Baptiste Carpentier.

L'activisme de l'École de guerre économique (EGE) et du Centre de recherche (CR) 451, sous l'impulsion de M. Harbulot, continue d'irriguer la pensée française sur l'intelligence économique. Y est développé le concept de « guerre économique » que M. Harbulot, à l'occasion d'une intervention récente, définissait comme « une confrontation entre parties pour capter, contrôler, accaparer des richesses, accroître sa puissance par l'économie », selon trois dimensions : « l'économie de guerre (modalités de politique industrielle affichée ou secrète), la guerre économique en temps de guerre (parasitage de l'économie de l'ennemi : pas de règles) et la guerre économique du temps de paix (modalités de sanctions économiques et dissimulation des stratégies d'expansionnisme commercial, de création de dépendance technologique, de déstabilisation d'économies émergentes) »[185]. M. Harbulot et M. Moinet notamment, qui depuis des années effectue, entre autres, un travail de conceptualisation de l'IE et de formation académique[186], estiment que la situation actuelle de guerre économique systémique (voir l'affrontement États-Unis – Chine) impose un pilotage stratégique par l'État qui permette de mieux prendre en compte la dimension « géoéconomique des échanges » et l'accroissement des « nouvelles formes de confrontation informationnelle », appelant ainsi à une mobilisation nationale.

En matière d'IE, la France n'est certainement pas démunie sur le plan conceptuel. Sur le plan pratique, elle dispose aussi d'entités performantes, dont les cabinets de conseil et d'IE, parmi lesquels l'ADIT, leader européen en la matière, dont certains estiment qu'il dispose de l'essentiel de l'information de sources ouvertes utile[187]. Cela étant, depuis des décennies, le milieu opérationnel de l'IE a été façonné par les cabinets anglo-saxons, de toute taille, qui ont essaimé leurs techniques, leur vision, leurs normes, et ainsi développé des réseaux très performants devenus incontournables, et dont une des missions est bien le renseignement économique compris comme la collecte d'informations mais aussi, et c'est un de leurs points forts, l'influence. Car lorsque l'on parle d'IE, on tend trop souvent à réduire

[184] CDSE, https://cdse.fr/le-cdse/, consulté le 3 décembre 2025.
[185] Christian Harbulot, *Intervention auprès du club des dirigeants de banques et établissements financiers d'Afrique et de la FAGACE (African Guarantee and Economic Cooperation Fund)*, BRED, 4 novembre 2025.
[186] M. Nicolas Moinet est Professeur des universités en sciences de l'information et de la communication à l'IAE de Poitiers.
[187] Source confidentielle.

celle-ci à une démarche de renseignement classique, souvent d'ailleurs erronément assimilé à l'espionnage, alors qu'il faut la comprendre comme une démarche globale focalisée sur l'information, qui combine observation, détection, captation, exploitation, anticipation et influence. M. Jean-Luc Angibault déplore ainsi « un rendez-vous manqué avec l'IE » dont la déclinaison des travaux conceptuels sur le plan opérationnel reste limitée, en raison en particulier de « la centralité quasi absolue de l'État, de la primauté de l'administratif sur l'opérationnel et d'un certain mélange des genres »[188].

Source : Cercle K2, mars 2025

Signalons qu'en matière d'IE, des divergences d'appréhension du concept existent entre services de renseignement : les uns insistent sur la spécificité des actions des SR que les grandes structures d'IE ne peuvent égaler, y compris l'ADIT, tandis que d'autres estiment que l'absence de coopération véritable entre des organismes comme l'ADIT et les SR est préjudiciable à l'économie française[189].

23 - Analyse critique : failles et insuffisances

Les constats, qu'il s'agisse de la menace ou du périmètre et des modes d'action de nos dispositifs (centraux et territoriaux) étant posés, il convient désormais de s'interroger sur la pertinence et l'efficacité de la démarche nationale.

Faisons-nous vraiment face à la menace dans toutes ses dimensions ?

En matière de pertinence et d'efficacité, comme vu précédemment, les récentes études ou rapports présentent des conclusions préoccupantes[190]. De même, de nos échanges avec des responsables de différents services de l'administration et certains acteurs économiques a émergé un questionnement partagé que l'on peut formuler ainsi : la France sait-elle ce qu'elle veut (quels objectifs atteindre et pourquoi), et a-t-elle dressé pour cela le véritable état des lieux de ses forces et faiblesses, en général

[188] Jean-Luc Angibault, « L'intelligence économique à la française est un rendez-vous manqué », *LinkedIn*, 22 octobre 2025.
[189] Affirmation non attribuable.
[190] Rapport d'activité 2022-2023 de la DPR ou Rapport Lienemann-Lemoyne sur l'intelligence économique de 2023, op. cit.

et dans les secteurs dits stratégiques, sachant qu'elle est soumise à des actions hostiles depuis des décennies qui ont amputé son potentiel et ses capacités ?

Si l'on ose regarder les choses en face, on conviendra du fait que les secteurs de pointe où la France peut encore jouer les premiers rôles sont nettement moins nombreux qu'il y a trente ans : disparition de secteurs entiers (technologies des télécommunications[191]), dépendances accrues (numérique, espace, technologies du solaire et de l'éolien), fragilisations (secteur automobile, notamment dans la filière électrique, nucléaire[192], énergie[193]). Et le défi pour rester en tête, particulièrement dans l'IA, le quantique, l'aéronautique ou le nucléaire est chaque jour plus redoutable.

Qui plus est, sous l'effet de la guerre en Ukraine depuis 2022 et de l'arrivée de l'administration Trump au pouvoir en janvier 2025, la compétition économique internationale ne fait que s'intensifier et se durcir. Or, à l'échelon central comme au niveau territorial, on remarque que les dispositifs actuels ont été pensés au cours des années 2010 et mis en place à compter de 2017-2019. Selon plusieurs interlocuteurs rencontrés, se présentent à nous deux difficultés. D'une part, le rythme d'évolution de nos dispositifs et pratiques. Certes, jusqu'au sommet de l'État, un constat lucide est posé sur la bascule du monde. Toutefois, dans les faits, la France dans son ensemble, son administration, ses entreprises et sa population, en a-t-elle pris la mesure ? Sur le terrain, la confrontation s'intensifie chaque jour, comme le confirme la région AURA, or la psychologie collective ne semble pas être au rendez-vous, tandis que les dispositifs de sanctions, y compris pénales, restent très timides, et qu'un certain réflexe européiste anime souvent l'administration dans la recherche de solutions, une manière peut-être de ne pas affronter le réel. D'autre part, le périmètre de notre action. Il est une question déstabilisante et provocante mais à notre avis salutaire posée en haut lieu qui consiste à se demander ce qu'il reste aujourd'hui à préserver en France. La perte par le passé de fleurons industriels ou l'érosion de notre avantage comparatif dans un certain nombre de secteurs laissent une France d'autant plus vulnérable qu'elle fait face à des appétits d'ogre et des puissances financières inégalables. Ne faudrait-il pas se recentrer sur certains secteurs stratégiques d'avenir tels que l'IA, le quantique, le nucléaire ou l'aéronautique, et peut-être le spatial, plutôt que de courir trop de lièvres à la fois ? Ne faudrait-il pas dresser un bilan objectif de notre retard technologique dans certains domaines (l'exemple de l'automobile électrique est révélateur) et développer des stratégies d'attractivité dont un des objectifs serait de capter en retour les technologies ainsi importées, à l'image de ce que font certains concurrents, la Chine et les pays émergents ?[194] Ainsi, il ne s'agirait pas tant de défendre que d'adopter une démarche proactive qui repose sur un constat lucide de nos forces et faiblesses évaluées à l'aune de la concurrence, actuelle et probable à moyen terme.

C'est peut-être dans une lecture classique et conformiste de la situation actuelle que réside la grande illusion française, celle qui voit dans l'ordre international hérité de l'Après-1945 un cadre immuable à faire vivre selon des règles intangibles. La France semble en effet avoir construit au fil des décennies passées un modèle économique dichotomique dont elle peine à sortir, constitué d'un côté de grands

[191] Tel est le cas emblématique du fleuron français Alcatel : fragilisation par les autorités américaines, fusion forcée avec l'Américain Lucent, puis rachat par le groupe finlandais Nokia.

[192] Guillaume Sarlat, *En finir avec le libéralisme à la française*, Paris, Albin Michel, 2015. L'auteur commente le cas d'Areva et de sa fusion en 2015 avec EDF, qui sanctionne une gestion décriée et témoigne d'une perte de compétitivité de la part d'un fleuron industriel français qui a par ailleurs largement contribué entretemps au développement de ses futurs rivaux, chinois notamment.

[193] Frédéric Pierucci, *Le piège américain*, Paris, Ed. J'ai Lu, 2020.

[194] On peut penser ici à nos partenaires israélien et coréen.

groupes pleinement intégrés au jeu du marché et suivant les règles de l'ordolibéralisme[195], jusqu'à l'excès, et, de l'autre côté, de l'ensemble des acteurs incapables de se jeter dans cette arène et placés dans l'orbite étatique sans pour autant qu'une véritable stratégie industrielle ait été définie[196]. À l'heure de la compétition internationale débridée et du nationalisme économique assumé, cette posture peut inquiéter.

Connaissons-nous vraiment l'état de la situation ?

Comme évoqué précédemment, le MEDEF s'interroge ouvertement sur la nécessité de mettre en place une structure de type observatoire qui serait chargée d'élaborer une cartographie précise de nos dépendances stratégiques et du risque économique, avec données et statistiques à l'appui, et ainsi d'orienter d'éventuelles actions et, idéalement, une véritable stratégie à l'échelle nationale. Chaque acteur économique connaît en effet l'état de ses dépendances, mais cela ne signifie pas pour autant, comme les Etats-Unis l'ont découvert à leurs dépens à l'occasion de la crise Covid (le niveau de dépendance, notamment vis-à-vis de la Chine, d'une partie du réseau de ses sous-traitants était inconnu du DoD[197]), que l'État ait une vision complète et précise à l'échelle de la nation de la situation en temps réel du tissu économique. Or, il ne peut y avoir d'action pertinente sans état des lieux documenté et suivi. Une telle initiative pourrait également contribuer à une meilleure information et sensibilisation de tous les acteurs concernés[198], ainsi qu'à l'élargissement du périmètre de travail dans la mesure où les efforts nécessaires et efficaces portés sur la BITD ne concernent qu'une partie minime, certes stratégique, de l'écosystème qui est par ailleurs soumis à une rude concurrence voire à des actions hostiles à fort impact sur l'état de santé général de l'économie française[199]. En d'autres termes, y a-t-il un focus excessif en France sur la défense nationale au détriment de secteurs non stratégiques mais dont les difficultés causées par des « manœuvres » étrangères (*cf.* Shein) peuvent, accumulées dans la durée, avoir un effet d'éviction et de ralentissement des performances de l'économie nationale ?

Avons-nous pris la pleine mesure des enjeux ?

Avons-nous véritablement compris, à tous les niveaux, l'enjeu central que représente l'information (données par exemple) et la dimension cognitive de l'affrontement économique systémique en cours ? Car une telle compréhension ne peut que se traduire par la mise en place de processus et de démarches de nature proactive et dynamique plutôt que protectrice ou défensive. Comme le souligne Nicolas Moinet, plutôt que « défense et attaque », il faut penser « réactif et proactif » car les notions d'attaque et de défense n'ont pas véritablement de sens dans le monde économique[200]. M. Harbulot parle, quant à lui, « d'encerclement cognitif par l'occupation du terrain par la connaissance » qui caractérise la compétition actuelle[201]. C'est pourquoi la fonction influence doit être pleinement intégrée à la démarche d'intelligence économique et plus largement de sécurité économique comprise comme une approche globale. En d'autres termes, nous sommes dans une « guerre de mouvement »,

---

[195] L'ordolibéralisme est un courant de pensée socioéconomique allemand d'essence libérale qui croit donc dans les vertus du marché mais prône la mise en œuvre de dispositifs de régulation, en particulier une certaine rigueur budgétaire, afin de garantir un ordre social aussi équilibré et juste que possible.

[196] Alexandre Devecchio, entretien avec Guillaume Sarlat, « L'autre triple A perdu : Alcatel, Alstom, Areva », *Le Figaro*, 3 juin 2015.

[197] Hélène Masson, Nicole Vilboux et Didier Gros, Rapport n°7, FRS, op. cit.

[198] Le MEDEF note que malgré les efforts actuels, les statistiques disponibles donnent à la majorité des acteurs économiques français l'impression que les difficultés rencontrées ne concernent que des secteurs particuliers et très minoritaires.

[199] Stéphanie Tison, entretien du 21 octobre 2025, MEDEF.

[200] Nicolas Moinet, entretien du 24 novembre 2025.

[201] Christian Harbulot, intervention BRED, *op. cit.*

comme l'affirme Nicolas Ravailhe, et il conviendrait de s'inspirer des méthodes de nos concurrents qui recourent à des stratégies ou tactiques de nature proactive[202] (Partie 3 – Recommandations).

La pertinence de notre organisation : peut-on parler d'une « équipe France » ?

La mobilisation de l'administration et des acteurs économiques est indéniable. La France dispose d'un véritable arsenal de « protection économique » et a depuis quelques années considérablement renforcé ses dispositifs et développé des compétences, l'adaptation des services de renseignement étant à ce tire révélatrice. Cependant, nous sommes tous témoins des assauts régulièrement subis par l'économie française sous la forme d'opérations de déstabilisation, de captation ou de prédation. Il convient donc de s'interroger sur la pertinence de l'organisation décrite supra.

De l'extérieur, certains spécialistes pointent la « fragmentation institutionnelle » comme obstacle à l'efficacité du dispositif français[203] tandis que d'autres constatent des « rivalités internes entre services de l'État » sur fond de lutte de pouvoir. Il est ainsi fréquemment noté que l'absence d'une chaîne décisionnelle qui puisse être identifiée et reconnue par tous les acteurs concernés nuit à l'efficacité du dispositif national[204].

La critique est aussi interne. Elle déplore de même la complexité de l'organisation générale qui se traduit par l'existence d'une multitude d'entités et d'interlocuteurs possibles pour les entreprises[205], l'hétérogénéité des dispositifs, le manque de coordination voire un défaut d'arbitrage et l'absence, là encore, d'une véritable « chaîne de commandement ». Est notamment soulignée la tension entre deux pôles « donneurs d'ordres » que sont l'Élysée d'une part et Bercy d'autre part, qui se traduit par des désaccords sur certains dossiers, en l'absence d'une véritable politique économique - ou a minima industrielle -, ajoutant ainsi à la confusion du processus décisionnel[206]. Plus précisément, une analyse critique récurrente concerne :

Le SISSE, qui joue certes un rôle éminent dans le dispositif de protection des actifs stratégiques français et a su s'imposer au cours des dernières années (mise en place réussie du guichet unique et reconnaissance par l'étranger). Si dans son rapport M. Roux de Bézieux a recommandé le maintien du SISSE en l'état, certains services du MEDEF demeurent circonspects en raison de sa taille trop réduite au regard des ambitions affichées et de son dispositif territorial encore trop fragile, relevant au passage que sa communication sur le nombre d'alertes a pour effet, aux yeux du « grand public » du monde économique (240 000 entreprises), de minorer l'importance de la menace qui ne concernerait qu'une maigre portion des entreprises françaises au sein des filières stratégiques. D'autres, au sein des SR en particulier, notent que malgré son rôle central et ses prérogatives définies par le décret du 20 mars 2019 (article 2, V), le SISSE, un service parmi tant d'autres au sein de Bercy, est limité à un rôle de protection et n'oriente ni ne pilote les SR dans les faits.

Les ressources humaines (RH) : le constat est fait d'une absence de culture économique au sein de l'administration en général[207], d'une insuffisance de communication entre les mondes économique et politico-administratif, et de l'étanchéité entre le monde du renseignement et l'Université. Pour preuve, contrairement à ce que l'on note chez nos partenaires-concurrents anglo-saxons, promoteurs dès les années 50 des « *intelligence studies*» dans les universités, les liens entre les

[202] Nicolas Ravailhe, entretien du 27 octobre 2025.

[203] Paolo Garoscio, « L'ingérence économique : une menace globale et insidieuse pour les entreprises », *Les carnets de l'économie*, 25 novembre 2024.

[204] Stéphanie Tison, MEDEF, *op. cit.*

[205] Source non attribuable.

[206] Ces « désaccords » peuvent porter sur le fond du dossier ; sur la forme, Bercy applique les éventuels arbitrages élyséens.

[207] Est ainsi pointé le défaut de véritable compétence économique au sein du cabinet du Premier ministre.

sphères publiques et privées demeurent ténus ; une traduction immédiate en est la difficulté pour les SR de recruter des profils économiques ou pour les entreprises de recruter des anciens membres des services, ce que la CIA, ou encore le FBI, font de manière « naturelle ». On citera ici l'exemple frappant et déconcertant d'une entreprise du CAC 40 ayant avoué préférer alerter la CIA plutôt qu'un service français en cas d'événement suspect en raison de la confiance inspirée par la réputation d'efficacité des services américains dans le domaine économique[208]. Tous les services ont fourni ces dernières années des efforts en matière de recrutement de profils économiques pour asseoir leur crédibilité et renforcer leurs compétences ; or, le bilan demeure insatisfaisant, sans doute aussi, comme le reconnaît l'un d'eux, parce que l'écosystème culturel français y est assez réfractaire d'une part, et parce que la dynamique économique française ne justifie pas toujours un investissement massif dans des compétences pointues d'autre part (recrutement de doctorants par exemple). Enfin, émanant de différentes sources, soit en administration centrale, soit au niveau territorial, un questionnement a été porté sur la pertinence des organisations RH d'acteurs majeurs de la « sécurité économique » tels que la DGA ou la DRSD dont les profils « militaires », en particulier chez la seconde, ne convainquent pas tous les acteurs du domaine.

Au-delà de ces remarques, c'est la cohésion de l'entreprise nationale qui est en jeu. L'observation des organisations, pratiques et comportements de nos principaux partenaires-concurrents fait ressortir l'existence d'un état d'esprit collectif fortement marqué par un sentiment d'appartenance nationale et de solidarité, c'est-à-dire de ce que l'on n'ose plus aujourd'hui appeler « patriotisme économique ». Ce dernier façonne les intérêts nationaux qu'il sert en retour, intérêts assumés et servis avec détermination, là encore, par tous les acteurs concernés[208]. Comme en témoignent nombre d'entretiens effectués, le constat n'est pas le même en France : pourquoi ? La France, marquée par son universalisme teinté de messianisme se voit-elle plus grande qu'elle n'est, et, face à ses difficultés, se projette-t-elle inconsidérément dans une vision européiste sublimée et compensatoire qui l'amène à se convaincre que l'Europe, et parfois même la « mondialisation heureuse », vaut bien quelques concessions nationales, fussent-elles stratégiques[209] ?

Ce constat des défaillances d'une équipe France toute théorique est formulé par de nombreux acteurs, à tous les niveaux de la chaîne de la sécurité économique. Des visions économiques parfois divergentes (comme évoqué précédemment entre l'Élysée et Bercy), les rivalités de pouvoir et de personnes favorisées par l'absence de pilotage reconnu et le « millefeuille administratif », les obstacles à l'émergence et à l'affirmation de start-ups françaises innovantes – et donc au potentiel de perturbation de l'écosystème établi élevé – posés, aussi surprenant que cela soit, par des grands groupes français eux-mêmes[210], ou encore le défaut de solidarité et de coopération en milieu international entre sociétés françaises confrontées à des difficultés communes sont autant de constatations et de réalités qui affectent nos performances, d'autant plus qu'elles sont parfaitement identifiées et exploitées par nos concurrents[211].

---

208 Fait rapporté non attribuable.

208 Les cas des Etats-Unis, de la Chine, de la Russie, mais aussi de l'Allemagne, de la Turquie, d'Israël et de bien d'autres encore sont patents.

209 En ce domaine, l'empressement des autorités françaises à appliquer les directives européennes est révélateur, jusqu'au moment, c'est-à-dire généralement tardivement, où l'on se rend compte qu'elles accroissent notre vulnérabilité (cas des CRSD).

210 Témoignage de la fondatrice d'une start-up française spécialisée dans des technologies innovantes et critiques.

211 Les Britanniques ont pour habitude de formuler cette boutade selon laquelle, lorsqu'il convient de mettre sur pied une entité multinationale, il est souvent pertinent d'en confier la direction à un Français car sa fidélité à la doxa internationale l'emportera largement sur son sens de l'intérêt national.

Le problème de fond est culturel. La « mère des batailles » est, sans doute, culturelle[212] (voir Partie 3 – Recommandations).

L'Union européenne : solution ou impasse ?

Très souvent, c'est en tout cas l'un des axes d'effort de la politique étrangère et européenne française depuis des décennies, la « solution UE » est mise en avant, comme la « sortie par le haut » qui permettra de compenser d'éventuelles faiblesses nationales et de favoriser l'émergence d'un écosystème « semi-fédéral » salutaire pour la puissance européenne en cours de consolidation. Le domaine qui nous intéresse n'échappe pas à ce réflexe national, pourtant piégeux.

Car l'UE est à la peine. Depuis la crise économique de 2008, son décrochage avec les Etats-Unis est patent, et très visible en France[213]. Ses dépendances technologiques se sont accrues (elle ne représente plus que 4% des brevets déposés dans le monde en 2024[214]) et les divergences entre États membres perdurent, sous pression américaine ou chinoise. Selon Nicolas Ravailhe, voir dans l'UE une « entité globale, mue par l'intérêt général commun », c'est ne pas regarder la situation en face[215]. Ainsi, le focus européen sur les FDI (Investissements étrangers en Europe), les alertes sur les domaines partagés ou les coopérations en matière de lutte contre la manipulation de l'information (LMI) relèveraient tout simplement d'une méthode ouverte de coordination entre États[216]. Dans les faits, l'UE est accessible et assez transparente, et certains partenaires encouragent cette posture dans la mesure où elle semble permettre de dynamiser l'économie et le commerce européens, ce dernier excédentaire, et d'en faire un atout dans le « grand jeu » économique international. C'est ainsi qu'alors que la France paraît s'arc-bouter sur des mesures de protection, l'UE de manière générale et l'Allemagne en particulier misent sur l'ouverture et une dynamique proactive. Les fonds européens, que nos concurrents font tout pour capter, ou encore les programmes d'innovation[217] portant parfois sur des domaines sensibles sont accessibles à des puissances étrangères car le pari est fait qu'il vaut mieux coopérer avec la Chine et les États-Unis par exemple dans une logique de « gagnant-gagnant » plutôt que de prendre des risques en érigeant des barrières face à ces puissances. D'une certaine manière, la porosité de l'UE renforce son attractivité et contribue à sa croissance, selon une lecture économique et non pas géopolitique. En cela, les approches française et allemande ou néerlandaise (voir l'effet Rotterdam[218]) divergent sensiblement, la première privilégiant la défensive, les secondes, dont les intérêts sont très croisés avec les Etats-Unis, mais aussi avec la Chine, jouant le jeu de la compétition, y compris au détriment de partenaires européens.

---

[212] Nicolas Moinet, séminaire de la Chaire du renseignement de l'IEP d'Aix-en-Provence, Paris, *op. cit*. Cette « thèse » est largement partagée par les spécialistes des questions de sécurité et d'intelligence économiques.

[213] Eurostat, Le PIB par habitant par région, en 2023 : La France compte désormais quatre régions parmi les plus pauvres de l'Est et du Sud de l'Europe.

[214] Natacha Polony, « Apocalypse UE ! », *L'Audace, op. cit*., p. 19.

[215] Nicolas Ravailhe, *op. cit*., p. 26.

[216] Nicolas Ravailhe, entretien du 27 octobre 2025.

[217] On notera que Huawei est présent dans un programme de recherche cyber de l'UE pour 242 millions d'euros, et que le cluster 4 du programme européen pour la recherche et l'innovation est ouvert à la Chine, https://www.horizon-europe.gouv.fr/sites/default/files/2024-02/guide-he-cl4-num-rique-call-2024-destinations-3-4-6-updated-pdf-10185.pdf, consulté le 8 décembre 2025.

[218] Il s'agit d'accepter un déficit commercial extérieur avec la Chine par exemple pour dégager un excédent intra-européen.

Le cas Vade Secure[219]

La pépite française en question, pourtant identifiée au plus haut niveau de l'État, s'est risquée à l'aventure américaine en 2014 et s'est vite retrouvée poursuivie en justice par la société Proofpoint, leader mondial. Reconnue coupable de détournement d'informations et de savoir-faire confidentiels, elle a été condamnée en 2023 à verser $14 millions. Fait étrange, Vade a été rachetée par le groupe allemand Hornetsecurity en mars 2024 ; or, ce dernier vient d'être lui-même racheté, après validation par les autorités françaises, par Proofpoint, laissant ainsi dubitatifs les experts qui ne peuvent s'empêcher de voir là une manœuvre concertée entre l'Allemagne et les États-Unis, ce qui ne serait d'ailleurs pas une première. La leçon à en tirer : *caute*, comme disait Spinoza.

L'appréciation du SGDSN est en l'occurrence instructive. Typiquement, les recommandations effectuées par le SGDSN au Premier ministre prennent en compte la dimension européenne puisqu'en matière de commerce, la hiérarchie des normes de l'UE s'impose à celle de la France. Par ailleurs, comme vu précédemment, l'UE s'est elle-même dotée d'une stratégie de sécurité économique et continue de prendre, dans ce domaine, un certain nombre de mesures qui complètent ou orientent les dispositifs nationaux, ou s'imposent à eux, le tout dans une certaine confusion dans la mesure où il n'existe pas de définition arrêtée et partagée de ce qu'est la sécurité économique[220].

Pour l'UE, les objectifs généraux de sécurité économique consistent à promouvoir les forces industrielles, à protéger les intérêts européens et à établir des partenariats avec des pays partageant les mêmes valeurs. Six domaines prioritaires à haut risque sont identifiés : réduire les dépendances stratégiques pour les biens et les services, attirer des investissements sûrs dans l'UE, soutenir une industrie européenne de la défense et de l'espace dynamique, ainsi que d'autres secteurs industriels critiques, garantir le leadership de l'UE dans le domaine des technologies critiques, protéger les informations et données sensibles et protéger les infrastructures critiques de l'Europe[221]. En complément, l'initiative *ResourceEU***,** très récemment annoncée, met l'accent sur « la lutte contre la dépendance excessive de l'Europe à l'égard des fournisseurs étrangers de matières premières critiques et de semi-conducteurs »[222].

Dans son arsenal, l'UE dispose en outre de quelques instruments potentiellement puissants qui pourraient être utiles à la France : son instrument anti-coercition[223], qu'elle s'est néanmoins interdit d'utiliser en réponse à l'imposition des droits de douane américains, ou encore son règlement de blocage, lequel toutefois ne fonctionne pas.

Par ailleurs, étendre à l'UE des mécanismes de protection nationaux n'est pas chose aisée. Comment ainsi envisager, par exemple, un dispositif de CIE au niveau de l'UE qui aurait sans doute pour conséquence première de faciliter les attaques en dévoilant des vulnérabilités ? Comment contrôler à ce niveau les investissements sortants, en miroir du *Reverse CFIUS* des États-Unis, sachant qu'il faudrait

[219] Adrien Lelièvre et Florian Dèbes, « French Tech : l'incroyable histoire de Vade, la start-up de cybersécurité rachetée par son pire ennemi », *Les Échos*, 16 mai 2025.
[220] SGDSN, entretien du 8 septembre 2025.
[221] Commission européenne, *Nouvelles mesures pour sécuriser les matières premières et renforcer la sécurité économique de l'UE*, 3 décembre 2025, https://commission.europa.eu/news-and-media/news/new-measures-secure-raw-materials-and-strengthen-eus-economic-security-2025-12-03_fr, consulté le 8 décembre 2025.
[222] Ibid.
[223] Parlement européen, *Instrument anti-coercition : la nouvelle arme de l'UE pour protéger le commerce*, UE, 21 septembre 2023, https://www.europarl.europa.eu/topics/fr/article/20230915STO05214/instrument-anti-coercition-la-nouvelle-arme-de-l-ue-pour-proteger-le-commerce, consulté le 8 décembre 2025.

avant tout s'entendre sur la définition d'un investissement, et que ce contrôle pourrait in fine desservir les intérêts économiques de l'UE ?

Enfin, l'UE peut être un obstacle via la prolifération de règlements plus vertueux les uns que les autres et qui, dans le contexte que l'on connaît, présentent in fine des contraintes et offrent des opportunités à nos concurrents. On citera le cas de la législation CRSD que la France, avec d'autres, remet en cause progressivement au motif que cet effort de normalisation handicape lourdement les entreprises européennes face à leurs concurrents, qui eux-mêmes, nous ne sommes plus à une contradiction près, ne manquaient pas de faire du lobbying pour les instituer…

Quelques démarches françaises vis-à-vis de l'UE : un impact encore difficile à évaluer

Le SISSE ne cache pas ses ambitions vis-à-vis de l'UE, qui s'articulent autour de trois axes : inspirer, en encourageant la mise en place de mécanismes de filtrage des investissements étrangers[224], influencer, en proposant des normes françaises et innover, en développant les échanges de renseignements et de procédures.

L'AFA cherche également à inspirer et influencer l'UE, son modèle de « contrôle a priori » étant original et de plus en plus reconnu par les acteurs étrangers.

Les SR, quant à eux, restent prudents. Ils notent les initiatives en cours au sein de l'UE en matière de sécurité économique mais notent par ailleurs la puissance d'influence des Etats-Unis comme de la Chine à Bruxelles. En matière de douanes, la France fait également figure d'exception car la DNRED ne peut que constater l'absence de culture douanière chez nombre de partenaires et la porosité des frontières européennes, donc les vulnérabilités ainsi créées, tout en estimant que l'enjeu européen ne peut être ignoré, et en appelant au renforcement des contrôles aux frontières.

En somme, la France n'est-elle pas victime d'un « verrouillage cognitif »[225] par rapport à l'UE, une somme de différentes stratégies économiques plutôt qu'un tout cohérent, qui brouille sa perception d'une réalité incompatible avec ses aspirations.

Quelle est la stratégie française ?

Dans une certaine mesure, nous payons aujourd'hui le prix de l'absence d'une véritable pensée stratégique en matière économique. C'est en substance le constat posé par le SGDSN face au durcissement de la compétition internationale et à ses conséquences, en particulier dans les domaines de la conformité, de la normalisation, et des actions de captation-prédation, autant de domaines qui depuis des décennies, aux Etats-Unis en particulier, font l'objet d'une réflexion, d'une « stratégisation » et d'actions résolues.

Que l'on parle de doctrine (le comment) ou de stratégie (l'articulation du « pour quoi » et du « comment »), les nombreux entretiens conduits mettent en relief un constat partagé : certes, une certaine idée de la sécurité économique est mise en avant, des efforts de mobilisation, de sensibilisation et de coordination sont entrepris, des mécanismes sont mis en place, mais l'ensemble n'est ni structuré (organisation) ni intégré dans une vision et un cadrage stratégiques appuyés sur un corpus « doctrinal » opératoire associant voies, moyens et objectifs en fonction d'intérêts identifiés, selon une logique de résultat.

En effet, la Commission « souveraineté et sécurité économiques des entreprises » du MEDEF note, d'une part, qu'il n'y a pas, contrairement à ce que l'on constate aux Etats-Unis, de consensus sur ce que l'on entend par « sécurité économique » et, d'autre part, qu'il n'y a pas de stratégie nationale ni

[224] Une telle disposition doit être renforcée par un nouveau règlement adopté en 2026.

[225] Nicolas Ravailhe, *L'Audace, op. cit*. p. 28.

de « pilote » pour coordonner l'ensemble des activités dans un but connu qui serve des intérêts bien identifiés. Ce constat est en partie partagé par certains services de l'administration qui révèlent des divergences d'approche en interne, évoquées précédemment, et l'absence dans les faits d'une superstructure décisionnaire qui mette en œuvre une stratégie nationale lisible. A été souligné le dilemme qui pèse sur l'économie française, c'est-à-dire le point d'interrogation sur l'équilibre à trouver entre « Choose France » et « Protect France », et la difficulté à s'accorder sur une feuille de route claire qui établisse des jalons et des objectifs communs. Plus largement, est pointé le décalage entre les ambitions affichées et les possibilités d'action, qui conduit à s'interroger sur la nécessité de revoir le périmètre de la sécurité économique, mais aussi ses modalités, dans une logique beaucoup plus proactive. Le dilemme évoqué supra est bien mesuré par d'autres organismes, notamment l'IHEDN, qui promeut une vision plus souple et proactive, considérant qu'il faut cesser de livrer des batailles d'arrière-garde et focaliser nos efforts sur les secteurs, voire les niches, de compétence et d'avenir en acceptant d'entrer dans une logique d'arsenalisation de l'interdépendance économique à notre profit, chaque fois que possible. Il faut, pour cela, une stratégie et une doctrine. On ne s'étonnera donc pas que la DGA, en particulier le service chargé de l'IE, abonde en ce sens.

Le « que veut-on, pourquoi et comment » (voir Partie 3 – Recommandations) fait défaut.

Un rôle pour le « grand public », le « grand oublié » ?

M. Harbulot parle d'une « cause sans peuple » lorsqu'il évoque, ce sont ses mots, le « pillage de l'économie française », et s'interroge sur l'absence de prise de conscience véritable par les citoyens de la situation critique de « guerre économique » dans laquelle leur pays se trouve[225].

Il n'est pas le seul. Un fossé semble s'être creusé, avec le temps, entre le jeu économique réel et la perception que peuvent en avoir les citoyens français, comme anesthésiés à la fois par les vertus tant vantées de la mondialisation et les bienfaits de l'État providence. Les phénomènes d'interdépendance économique sont compris et admis, et souvent acceptés comme autant de dynamiques vertueuses, sans distinction de nature (cas des secteurs stratégiques par exemple). La crise de la Covid-19 a certes ébranlé cette confiance aveugle et a permis de sensibiliser la population à la dureté des rapports économiques et aux conséquences parfois fâcheuses de certaines dépendances volontairement souscrites… Mais il n'est pas sûr que les citoyens mesurent la rigueur de la lutte quotidienne qui oppose les puissances et les acteurs économiques sur la scène internationale, une lutte trop souvent réduite à un affrontement entre la Chine et les Etats-Unis dont on peine à voir, ou à vouloir voir, les véritables conséquences, actuelles et probables à terme. Peu d'entre eux mesurent les dégâts financiers et humains causés par certaines actions hostiles, peu imaginent qu'elles proviennent majoritairement de nos plus proches alliés et partenaires, peu font le lien entre leur situation quotidienne et ces dernières. Dans un contexte socioéconomique national tendu, comme l'ont démontré certaines réactions au récent discours du chef d'état-major des armées devant le Congrès des maires[226], partager des considérations et des faits de nature anxiogène n'est pas chose aisée, et requiert sans doute autant de finesse d'approche que de détermination. Or, éduquer et sensibiliser est un impératif.

Se pose donc la question de la communication, au sens d'une diffusion plus large et plus régulière d'informations à l'attention du grand public. Ce questionnement est partagé par beaucoup des acteurs rencontrés qui estiment que la démarche française, y compris d'ailleurs vis-à-vis des PME par exemple, pourtant au cœur de nos préoccupations, demeure trop confidentielle, trop élitiste, trop distante. En ce domaine, le fait que le rapport de Bézieux soit resté confidentiel est déploré par tous les experts de

[225] Christian Harbulot, *La guerre économique, une « cause sans peuple ?* », École de pensée sur la guerre économique, 27 octobre 2025.
[226] Général Mandon, « *Discours aux maires* », 107ème Congrès des maires, Paris, 18 novembre 2025.

ces questions qui estiment que cette démarche est contreproductive et va à l'encontre de l'objectif de « mobilisation nationale », le « tour de France » de l'ex-président du MEDEF n'intéressant majoritairement que des personnes déjà convaincues et au fait des problématiques exposées[227].

Des éclairages spécifiques révélateurs du durcissement de la compétition

Le Lawfare *: le droit, une arme comme les autres*

L'auteur de cette étude, alors en fonctions au SGDSN, de retour des États-Unis, avait organisé une réunion inaugurale sur le thème des menaces hybrides, en prévision de la mise sur pied d'un groupe de travail (GT) interministériel (IM) sur les menaces hybrides (MH), et choisi parmi les premiers thèmes à évoquer le *lawfare*. En amont de la réunion, nos experts nationaux avaient été sollicités sur le sujet (définition, compréhension française des enjeux, etc.). Il avait été frappé, à cette occasion, de constater le degré d'ignorance, non pas des experts eux-mêmes, très qualifiés, mais du « grand public » de l'administration, indifférent aux enjeux du domaine parce que mal informé.

Depuis, les choses ont eu l'heur d'évoluer dans le bon sens puisque ce GT a été pérennisé d'une part, et le volet *Lawfare* considérablement développé d'autre part. Depuis 2020, un rendez-vous annuel formel réunit les acteurs du domaine qui agissent selon trois axes. Premièrement, la dimension normative, qui concerne principalement les législations extraterritoriales. Dans ce domaine, l'adversaire historique sont les Etats-Unis, mais aujourd'hui la Chine, via ses législations sur le contrôle des exportations, cherche à faire jeu égal. Le champ normatif est sans cesse plus actif et est une des voies privilégiées pour la captation de données, d'autant que plusieurs domaines ne sont pas encore véritablement régulés (cyber, IA, espace exo-atmosphérique, etc.). Deuxièmement, le contentieux, qui vise, par exemple, à utiliser les juridictions internationales (CIJ, CPI, CEDH) pour assigner en justice un pays qui contreviendrait à ses obligations (cas de la plainte déposée devant la CIJ par la France contre l'Iran pour « violation du droit à la protection consulaire »)[228]. Troisièmement, la stratégie d'influence, qui a pour objet l'édiction de la norme. Un des enjeux réside dans la mobilisation des partenaires privés et publics compétents ainsi que dans la définition des secteurs stratégiques à privilégier.

La DPR l'affirme ainsi : « Le renseignement doit contribuer à identifier, dénoncer, voire entraver les actions malveillantes et les actions d'influence faussant l'environnement juridique et normatif des acteurs économiques. La création du parquet national financier et de l'Agence française anticorruption puis la loi Sapin II, ont répondu en partie à cette épée de Damoclès dirigée vers nos actifs les plus stratégiques. Pourtant, le risque demeure et il faut être vigilant à ce que certains cabinets de conformité anglo-saxons actifs au sein d'entreprises sensibles ne transfèrent pas hors de France les informations critiques auxquelles ils ont accès »[229].

La France n'ignore pas le champ de bataille du *lawfare* et s'est dotée (ou a réactivé) un certain nombre de dispositifs en conséquence.

Il s'agit tout d'abord de la loi dite de « blocage » de 1968, amendée en 1980, 2002 puis 2022[230] : ce dispositif est abusivement qualifié de « loi de blocage » par nos concurrents anglo-saxons, alors qu'il

[227] Stéphanie Tison, MEDEF, entretien du 21 octobre 2025.

[228] Dans le cadre de l'affaire Cécile Kohler et Jacques Paris, otages aujourd'hui libérés.

[229] DPR, 2022-2023, *op. cit*.

[230] JORF, Loi n° 68-678 du 26 juillet 1968 relative à la communication de documents et renseignements d'ordre économique, commercial, industriel, financier ou technique à des personnes physiques ou morales étrangères, https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326, consulté le 30 septembre 2025. Les amendements de 1980 et 2002 sont marginaux et stipulent en particulier les peines encourues au pénal et sur le plan financier. La « réforme » de février et mars 2022 vise à simplifier les procédures pour les entreprises (SISSE comme guichet unique) et à renforcer l'opposabilité de la loi vis-à-vis des juridictions étrangères.

s'agit d'une loi de « filtrage » et d'« aiguillage », un instrument juridico-diplomatique qui permet de justifier la non-communication d'informations. Son article I mérite d'être cité en intégralité : « *Sous réserve des traités ou accords internationaux, il est interdit à toute personne physique de nationalité française ou résidant habituellement sur le territoire français et à tout dirigeant, représentant, agent ou préposé d'une personne morale y ayant son siège ou un établissement de communiquer par écrit, oralement ou sous toute autre forme, en quelque lieu que ce soit, à des autorités publiques étrangères, les documents ou les renseignements d'ordre économique, commercial, industriel, financier ou technique dont la communication est de nature à porter atteinte à la souveraineté, à la sécurité, aux intérêts économiques essentiels de la France ou à l'ordre public, précisés par l'autorité administrative en tant que de besoin* »[231]. Une seule condamnation a résulté de la saisine du guichet interministériel en 2007, dans le dossier Executive Life[232]. De l'aveu même du SISSE, le texte est constitutionnellement fragile et, dans les faits, peu dissuasif[233] dans la mesure où, contrairement à ce qu'il se passe chez plusieurs de nos concurrents principaux, la loi ne comprend pas de mécanisme de sanction en cas d'infraction commise par une entité étrangère (espionnage, audit manipulé, etc.)[234]. Toutefois, dans certains cas, son efficacité tend à se renforcer dans la mesure où davantage de juridictions étrangères (cas de la décision Virginia Foley en 2025 aux Etats-Unis) reconnaissent son applicabilité [235] .

Un autre instrument majeur est la loi Sapin II[236] : « La loi du 9 décembre 2016 sur la transparence, la lutte contre la corruption et la modernisation de la vie économique, dite « Sapin II », a pour objectif une modernisation en profondeur de la législation française dans le respect de principes reconnus au niveau international. Parmi les points majeurs à retenir de la loi au titre I « de la lutte contre les manquements à la probité », figurent « L'obligation générale de prévention et de détection de la commission, en France ou à l'étranger, des faits de corruption ou de trafic d'influence ; la protection des lanceurs d'alerte ; l'introduction dans le Code de procédure pénale d'une disposition permettant de conclure une convention judiciaire d'intérêt public ; la création d'une Agence française anticorruption (AFA) : le Service central de prévention de la corruption – SCPC, créé dans le cadre de la loi Sapin 1 n° 93-122 du 29 janvier 1993 – est remplacé par l'Agence française anticorruption, dotée de prérogatives étendues ; l'extraterritorialité de la loi française en matière de délits de corruption et de trafic d'influence actifs et passifs ». Le niveau d'exigence ainsi fixé est élevé, mais il constitue un gage de professionnalisme et de protection renforcée par rapport aux ingérences, sous la forme d'accusations de corruption, menée par des puissances étrangères en vertu de l'extraterritorialité de leur droit. L'Agence Française Anti-corruption (AFA), dont il faut bien reconnaître que la création a été décidée en partie sous pression de l'OCDE, vise justement à l'origine à se protéger des ingérences américaines et à renforcer la souveraineté française. Elle impose un certain nombre de dispositifs anti-corruption organisés autour de huit mesures à mettre en place par les entreprises de plus de 500 employés et d'un chiffre d'affaires (CA) supérieur à 100 millions d'euros, qu'elles soient privées ou publiques (sans sanction possible pour ces dernières)[237]. L'AFA agit donc en prévention et, par ses audits et instruments de contrôle, contribue à renforcer l'écosystème français, à le crédibiliser face à ses concurrents internationaux, et à le protéger d'ingérences éventuelles[238]. L'AFA cherche aujourd'hui

---

231 *Ibid.*

232 Cette affaire, initiée par le rachat, jugé non conforme aux lois locales, d'une compagnie d'assurance-vie californienne en 1991 par le Crédit Lyonnais, ne sera close qu'en 2012, après l'imposition de sanctions et pénalités financières pour un montant de 600 millions de dollars en 2005.

233 Six mois d'emprisonnement et 18 000 euros d'amende.

234 SISSE, entretien du 10 septembre 2025.

235 Olivier Attias, Laura Bol, Discovery américaine et ordre public français : refus d'exequatur, August Debouzy, 17 mars 2026.

236 Loi n° 2016-1691 du 9 décembre 2016 relative Ã la transparence, Ã la lutte contre la corruption et Ã la modernisation de la vie economique, https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000033558528, consulté le 28 novembre 2025.

237 Il s'agit de : cartographie, formation, conduite, discipline, comptabilité, alerte, évaluation des tiers et évaluation interne.

238 10 à 15 contrôles par an et 70 opérations de sensibilisation effectuées partout en France en 2024.

à consolider sa réputation au sein de la communauté internationale et à améliorer, par un accompagnement adapté, le niveau de sensibilisation des PME en particulier, souvent confrontées à l'obligation de mettre en place des dispositifs lourds et coûteux. Notons enfin, dans le cadre de la loi du 9 décembre 2016, l'institution de la Convention judiciaire d'intérêt public (CJIP), inspirée de la procédure de *Deferred Prosecution Agreement* (DPA) des Américains et Britanniques. La CJIP permet ainsi de contrer les ingérences étrangères grâce à un dispositif de sanctions[238], de prévention de la récidive par la mise en conformité sous contrôle français plutôt qu'étranger, et de mécanismes de coopération multilatérale, notamment avec la partie américaine.

S'ajoute à ces dispositifs le parquet national financier (PNF), créé le 6 décembre 2013, qui est un « parquet à compétence nationale spécialisé, en charge de la grande délinquance économique et financière. Il traite les atteintes aux finances publiques, à la probité, au bon fonctionnement des marchés financiers et, depuis 2020, au jeu libre de la concurrence »[239]. On relèvera qu'à l'occasion de son audition[240] en 2023 devant la Commission d'enquête relative aux ingérences politiques, économiques et financières de puissances étrangères – États, organisations, entreprises, groupes d'intérêts, personnes privées – visant à influencer ou corrompre des relais d'opinion, des dirigeants ou des partis politiques français, M. Bohnert, Procureur de la République financier, déclarait que de la notion d'ingérence, bien que non « appréhendée en tant que telle par le droit pénal » peuvent se rapprocher « certaines qualifications d'atteinte aux intérêts fondamentaux de la nation, notamment les crimes et délits qui figurent aux articles 411-4 et 411-5 du Code pénal, regroupés dans la section intitulée « Des intelligences avec une puissance étrangère ». Il soulignait le rôle des Etats-Unis qui, par le biais du *Foreign Corrupt Practices Act* (FCPA), avaient pu engager 488 actions entre 1977 et 2015. Statistiquement, le PNF constate que pour les dix sanctions les plus importantes prononcées au titre de la loi de 1977, le montant des amendes se situe entre 585 millions de dollars et 3,3 milliards de dollars, et que les entreprises visées sont principalement européennes – trois françaises, deux suédoises, une allemande et une néerlandaise – contre une entreprise américaine et une brésilienne. Le constat est donc sans appel : « Ces affaires traduisent très clairement une ingérence du droit américain en direction des entreprises françaises. Pour compléter ce panorama, il faut y ajouter la sanction de 9 milliards de dollars prononcée en 2014 contre BNP pour violation d'embargo »[241].

Mentionnons enfin la création, par la loi du 11 octobre 2013, de la Haute autorité pour la transparence de la vie publique (HATVP)[242], une autorité administrative indépendante veillant à s'assurer de la probité de la vie publique. Cet instrument sert à asseoir la crédibilité de l'administration publique française, par sa fonction de régulation de la représentation d'intérêts. Il aura toutefois fallu attendre le 1er juillet 2025 pour qu'elle prenne en compte la problématique de l'influence étrangère.

Ainsi, les travaux se poursuivent, en France et en Europe. Sur le plan juridique, face aux mesures à portée extraterritoriale, un enjeu déjà mis en relief par le rapport Gauvain du 26 juin 2019[243], l'arsenal s'est consolidé ; on signalera le vote de la loi n° 2024-850 du 25 juillet 2024 visant à prévenir les ingérences étrangères en France[244], complétée par le Décret n° 2025-733 du 31 juillet 2025 relatif à la

[238] 5 milliards d'euros avaient depuis été versés au Trésor public à la date de l'audition.
[239] PNF, https://www.justice.gouv.fr/actualites/actualite/dix-ans-daction-du-parquet-national-financier, consulté le 10 décembre 2025.
[240] Assemblée nationale, Compte-rendu d'audition à l'Assemblée nationale, 16 juin 2023, Compte rendu de réunion n° 11 - Jean-François Bohnert, Procureur de la République financier, 16 juin 2023.
[241] *Ibid.*
[242] JORF, Loi n° 2013-907 du 11 octobre 2013 relative à la transparence de la vie publique, 12 octobre 2013.
[243] https://www.vie-publique.fr/files/rapport/pdf/194000532.pdf, consulté le 10 décembre 2025.
[244] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000050052193, consulté le 10 décembre 2025.

transparence des activités d'influence réalisées pour le compte d'un mandant étranger[245]. En Europe, il existe, depuis 1996, un « outil de blocage », le règlement 2271/96 du 22 novembre 1996 portant protection contre les effets de l'application extraterritoriale d'une législation. Ce règlement permet d'indemniser les opérateurs victimes des instruments extraterritoriaux et leur interdit de se conformer aux éventuelles sanctions décidées par un État tiers. Cette « loi de blocage » a été amendée et élargie en 2018.

Nonobstant ces dispositifs juridiques, force est de constater que la « bataille de l'extraterritorialité » est plus féroce que jamais, comme l'atteste la dynamique chinoise par exemple. La « guerre par le droit » sévit selon les axes précédemment évoqués (normalisation, contentieux et influence) dans tous les champs de l'activité économique, et représente à ce titre un enjeu majeur de pouvoir et de souveraineté intrinsèquement lié, il faut bien le reconnaître, à la puissance effective des acteurs qui en usent voire en abusent. Dans ce domaine comme dans d'autres, le poids relatif et la « force » tendent à s'imposer.

La cybersécurité ou la quadrature du cercle

Si l'on prend comme référence la classification par les armées françaises des milieux (espaces terrestre, maritime, aérien, extra-atmosphérique et cyber) et des champs (espaces informationnel et électromagnétique)[246], le « cyber » est au croisement d'un milieu et d'un champ, en l'occurrence informationnel. Il est à la fois domaine et vecteur de « menaces » liées à la sécurité des systèmes et à la gestion des données et informations.

La cybermenace est en conséquence généralement répertoriée comme une menace à part entière en matière de sécurité et d'intelligence économiques tant son déploiement et ses effets se sont accélérés et démultipliés au fil du temps, comme le confirme la directrice de la DGSI. Sur le plan des ingérences, l'outil cyber est en effet au cœur de nombreuses stratégies, tactiques ou procédures à des fins de captation, de prédation, de désinformation ou d'attaque réputationnelle pour ne citer que quelques applications possibles.

Dans ce contexte, la cybersécurité est rapidement devenue un enjeu de sécurité et de souveraineté nationale. Ceci explique les efforts considérables accomplis ces dernières années pour renforcer la résilience de nos entreprises et des systèmes d'information associés, dans le but de maintenir sous contrôle l'information ou la donnée, cible première des acteurs de la « guerre économique », en particulier dans les secteurs stratégiques. L'écosystème français s'est donc consolidé, sous l'impulsion des autorités gouvernementales successives, via l'Agence nationale de la sécurité des systèmes d'information (ANSSI) d'une part, et un ensemble d'acteurs privés d'autre part, spécialisés dans ces technologies. La France publie ainsi régulièrement des stratégies et des documents d'emploi au profit des entreprises, travaille de concert avec ses partenaires européens au renforcement des systèmes face aux partenaires-concurrents extra-européens[247], et s'attache à développer une culture de la cybersécurité à tous les échelons, en administration centrale et territoriale, et au sein des entreprises voire du grand public. C'est ainsi que la France, dans un contexte de « massification de la menace »[248],

[245] https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000052018706, consulté le 10 décembre 2025.
[246] Centre Interarmées de Concepts, de Doctrines et d'Expérimentations-CICDE, *Multimilieux et multichamps (M2MC), la vision française interarmées*, concept interarmées CIA-0.1.1_M2MC(2021), Ministère des Armées, 6 septembre 2021.
[247] Il s'agit notamment des directives NIS (*Network and Information Security*).
[248] ANSSI, *Plan stratégique de l'Agence nationale de la sécurité des systèmes d'information 2025-2027*, mars 2025, file:///C:/Users/ddrgr/Downloads/Plan-strat%C3%A9gique-2025-2027-de-lANSSI%20(1).pdf, consulté le 26 septembre 2025.

dispose d'un plan stratégique en matière de cybersécurité[249] ou encore de différents dispositifs de protection et d'intervention active tels que les CERT et CSIRT, complétés par des équipes mobiles chargées d'intervenir au profit d'acteurs attaqués ou vulnérables.

Pourtant, la polémique sur les capacités françaises et le niveau réel de protection de nos systèmes ne désenfle pas. Par-delà le constat fait par certains SR du niveau toujours préoccupant en matière de cybersécurité au sein des entreprises, ce malgré les investissements humains et matériels déployés, force est en effet de constater que l'idéal de « souveraineté numérique » demeure un idéal, et que les vulnérabilités françaises, à la fois culturelles et techniques, peinent à se résorber. La raison première est connue de tous : il s'agit du retard accumulé par la France, et la plupart des acteurs européens d'ailleurs, dans le domaine cybernétique face aux Etats-Unis et aux systèmes qu'ils ont conçus et déployés partout dans le monde, via les GAFAM et la *New Tech* aujourd'hui. La France et l'UE sont devenues, inexorablement, dépendantes, profondément bien qu'à des degrés divers et variables, de l'Amérique. Notre architecture cyber nationale repose en effet sur des technologies et des systèmes américains ; une telle situation, conjuguée aux ingérences constatées de la part de notre puissant allié, donne la mesure de notre vulnérabilité. Partant de ce constat, les avis divergent. Les uns considèrent qu'il est urgent et impératif de se doter de systèmes et d'une architecture « *made in France* » ou, éventuellement, « *made in Europe* », c'est-à-dire de s'émanciper de Microsoft, Google et autres, et de leurs « *clouds* », pour développer un système d'exploitation (OS-*Operating System*) souverain[250]. Ils constatent en effet que l'immense majorité des services de l'administration, des ministères, mais aussi des écoles, universités et centres de recherche fonctionnent avec Microsoft 365, et sont donc vulnérables par le biais du recours à d'éventuelles « *backdoors* », et placés sous l'épée de Damoclès du US *Cloud Act*. En l'occurrence, les déclarations récentes du directeur des affaires publiques et juridiques de Microsoft France, qui reconnaît qu'il ne pourrait s'opposer à une demande d'accès aux données de la part des autorités américaines en vertu du *Cloud Act*, ne font que les conforter dans leur analyse[251]. Les autres, notamment les responsables de ce domaine au sein de l'ANSSI et du SGDSN, estiment cette ambition déraisonnable. Pour eux, il est trop tard pour construire les fondations d'un nouvel édifice national, d'autant que, n'en déplaise à notre égo, les compétences américaines sont remarquables et difficilement remplaçables ; il faut au contraire investir dans des dispositifs complémentaires sécurisés et étanches aux ingérences étrangères, qu'elles soient conduites par des voies techniques ou par l'extraterritorialité du droit[252].

Aujourd'hui, en France, les dispositifs européens de type NIS 1 sont appliqués et permettent de renforcer la protection des installations et infrastructures sensibles. La transposition en droit français de la directive NIS2, une directive que la France a activement contribué à élaborer, pour l'instant en suspens dans les limbes parlementaires, devrait à terme permettre de renforcer la cybersécurité. En parallèle, l'ANSSI a mis au point un dispositif novateur, l'offre SecNumCloud, une certification qui, selon les dires de son directeur, garantit l'étanchéité du système ainsi certifié aux lois d'extraterritorialité[253], tout en offrant une protection technique de haut niveau. La notion d'étanchéité

[249] ANSSI, *Ibid*.

[250] Tel est l'avis par exemple de M. Jean-Florian Bacquey-Roullet, spécialiste des question cyber et fondateur de BRDev, une structure de consultance et de formation, et intervenant auprès du MESR.

[251] Aymeric Geoffre-Rouland, « La France ne contrôle plus ses données : Microsoft les remettra aux États-Unis "si nous y sommes contraints" », analyse des propos de M. Anton Carniaux, directeur des affaires publiques et juridiques de Microsoft France au Sénat, 10 juin 2025, https://www.lesnumeriques.com/societe-numerique/la-france-ne-controle-plus-ses-donnees-microsoft-les-remettra-aux-etats-unis-si-nous-y-sommes-contraints-n240010.html, consulté le 29 août 2025.

[252] Jonathan Collas, Conseiller Industrie et numérique, Entretien, SGDSN, 7 novembre 2025.

[253] La certification impose par exemple que la direction des opérations juridiques ne soit pas sous autorité américaine. Elle est conçue dans un environnement juridique strictement européen.

continue toutefois de faire débat. M. Luc Julia affirme ainsi que l'ANSSI « donne des tampons « souverain » à des *clouds* qui ne le sont pas du tout [S3NS et Blue en l'occurrence] » et, en parlant des données en question, que « la NSA y a accès »[254]. Par ailleurs, les échanges du printemps 2025 entre le directeur de l'ANSSI et les sénateurs de la commission d'enquête du Sénat sur la commande publique ont mis en relief les tensions existantes[255] : en effet, les exigences techniques de SecNumCloud étant très élevées, elles ne seront pas accessibles à la plupart des administrations ou entreprises[256], tandis que le droit européen lui-même, en raison des divergences politiques internes à l'UE, n'est pas une garantie absolue face aux attaques par le droit de la part des Américains notamment. Il faut le rappeler, l'architecture technique de nos systèmes repose, y compris dans le cas de logiciels développés par des entreprises françaises, en partie sur des fondations techniques américaines. La prise en compte de cette réalité a d'ailleurs conduit Thalès à opter pour une offre *cloud* mixte[257] dite S3NS[258], en partenariat avec Google, tout en obtenant la certification SecNumCloud, tandis que Orange et Capgemini ont opté pour le système *cloud* Bleu[259], en partenariat avec Microsoft. À moyen terme, la DINUM travaille à sa « Suite Numérique », un ensemble de fonctionnalités (messagerie Tchap, outil de visioconférence Visio, etc.) qui permettrait l'utilisation, au quotidien, d'outils « souverains » par l'administration publique.

Quoi qu'il en soit, la réalité est celle d'une « France cyber » non souveraine, qui a vu son projet EUCS[260] (certification européenne de cybersécurité du *cloud* ou *European Union Cybersecurity Certification Scheme for Cloud Services*) être rejeté ou plutôt dévoyé par l'UE, sous l'impulsion de l'Allemagne, elle-même sous pression des États-Unis[261]. Elle est donc aujourd'hui engagée dans une démarche active de protection et de résilience afin de limiter au maximum les effets de la dépendance technologique et d'encourager ce faisant le développement de compétences nationales[262]. Il s'agit, en quelque sorte, de généraliser une offre certifiée la plus sécurisée possible, selon une logique de « prêt-à-porter » accessible à tous[263].

Le défi n'est pas mince, pour plusieurs raisons. La première concerne la nature de l'offre française, à la fois fragmentée, comme le reconnaît le directeur de l'ANSSI, et donc moins efficace face à l'offre américaine conçue, comme toujours, selon une approche pragmatique. La seconde concerne la dépendance technologique structurelle et dévoile un paradoxe, là encore sous-entendu par l'ANSSI : les compétences techniques françaises sont présentées comme désormais d'un niveau comparable à celui des entreprises américaines, et pourtant notre dépendance perdure, faute sans doute de consolidation capitalistique suffisante, mais aussi d'une filière française de cybersécurité encore sous-

[254] Natacha Polony et Luc Julia, « entretien avec Luc Julia », *L'Audace, op. cit.*, p. 102.
[255] Audition de M. Vincent Strubel, Directeur général de l'ANSSI, Sénat, le 28 mai 2025.
[256] Au cours de cette audition, les cas du marché de l'UGAP remporté par Microsoft alors que dès 2015 un accord de coopération avait été mis en place avec l'ANSSI, et celui du Health Data Hub remporté en 2019 par l'offre américaine face à des offres françaises au coût trop élevé, ont été évoqués.
[257] Il s'agit de développer des *clouds* souverains pour lesquels les entreprises américaines fournissent les technologies mais ne « voient » pas les données. Ni le US *Cloud Act* ni les dispositions du FISA ne peuvent s'appliquer.
[258] Thalès, « S3NS accélère son développement vers le cloud de confiance », communiqué de presse, 29 avril 2025.
[259] Gabriel Thierry, « Les retards à l'allumage de Bleu, l'offre cloud de Capgemini, Orange et Microsoft », *La Lettre*, 18 février 2025.
[260]CNIL, « Cloud : les risques d'une certification européenne permettant l'accès des autorités étrangères aux données sensibles », 19 juillet 2024.
[261] Jonathan Collas, Entretien, SGDSN, 7 novembre 2025.
[262] *Ibid*. On citera OVHcloud, Clever Cloud ou encore Linagora.
[263] *Ibid.*

dimensionnée par rapport à nos ambitions, en raison d'un manque d'attractivité et de difficultés de recrutement[264]. Enfin, la charge financière et administrative de la mise en œuvre des seules dispositions NIS pour les ETI, PME et TPE devra faire l'objet d'aménagements pour être supportable à terme.

[264] Vincent Strubel, audition au Sénat, *op. cit*. L'ANSSI serait en déficit de 50 à 60 ETP (Equivalents Temps-Plein).

Partie 3 – Recommandations – Lignes d'opérations

Dans leur rapport de 2023, les sénateurs Lienemann et Lemoyne appellent à une « révolution » culturelle et organisationnelle. Leur proposition clé est de « confier à un Secrétariat général à l'intelligence économique rattaché au Premier ministre l'élaboration en interministériel d'une stratégie nationale d'intelligence économique »[265] ; elle se décline ensuite par un arsenal de vingt-deux mesures visant à en faire un outil de cohérence et d'efficacité au profit de l'intérêt général, « afin que l'État, les collectivités territoriales, les établissements de recherche, les entreprises et les citoyens soient davantage en état d'alerte sur les rapports de force économiques à l'œuvre aujourd'hui dans le monde et mieux armés pour y faire face »[266].

Nos conclusions et recommandations s'inscrivent dans cette approche. Toutefois, bien que le rôle de la fonction intelligence économique ne saurait être minoré puisqu'elle est la condition de la juste compréhension des menaces, défis et enjeux qui nous intéressent, nous considérons qu'il faut élargir la focale à partir du concept de sécurité économique. Celui-ci comprend, répétons-le, deux dimensions : il est indissociable du concept de sécurité nationale, donc consubstantiel au concept de souveraineté nationale d'une part, et il constitue d'autre part un champ d'action où les acteurs nationaux, organisés en conséquence, mettent en œuvre leurs capacités selon des modalités réactives et proactives, en vue de garantir la protection et la promotion d'intérêts stratégiques identifiés, mais aussi de façonner des opportunités.

C'est pourquoi nous plaçons au centre de notre réflexion et des préconisations de l'étude le projet d'établissement d'une véritable stratégie de souveraineté et de sécurité économiques qui permette de définir et de relier l'intention politique à l'action opérationnelle, dans une logique de cohérence et de recherche d'efficacité assumée.

31 - Un référentiel pour une stratégie de souveraineté et de sécurité économiques

Au terme de cette étude, il nous a paru pertinent de proposer un modèle de réflexion stratégique pouvant conduire à l'élaboration d'une stratégie nationale (voir le schéma de l'articulation entre intérêts, objectifs et menaces/opportunités, p. 69). Ce modèle, à vocation pédagogique ou du moins illustrative, ne prétend pas servir de référentiel absolu à la démarche suggérée. Il fournit toutefois un cadre, une matrice, et dessine un chemin, à partir des éléments d'analyse recueillis au cours des six mois passés, qui permettent d'ouvrir des perspectives, sous la forme de pistes de réflexion et d'action que nous pensons utiles à la maturation d'un projet national.

Certaines rubriques sont volontairement sommaires dans la mesure où elles font directement référence au matériau contenu dans cette étude. D'autres sont plus fournies à des fins d'explicitation de la démarche proposée.

Des présuppositions

Celles-ci fondent la pertinence de la démarche, et doivent elles-mêmes être révisées régulièrement pour garantir la validité de l'exercice dans le temps. Dans le cas qui nous occupe, nous

[265] Rapport Lienemann-Lemoyne, op. cit., https://www.senat.fr/rap/r22-872/r22-8720.html#toc0, consulté le 23 juin 2025.
[266] *Ibid.*

proposons quatre exemples de présuppositions pouvant guider et structurer une réflexion stratégique :

Le paradigme paix-crise-guerre n'est plus pertinent. Notre grille de lecture doit évoluer et intégrer la conflictualité permanente comme l'hybridité des actions et des acteurs. En ce sens, le nouveau triptyque « compétition-contestation-affrontement » mis en avant dès 2021 par le général d'armée Thierry Burkhard, ancien chef d'état-major des armées françaises, prend tout sa pertinence.

La sécurité économique est aussi affaire de sécurité nationale. Le contexte géopolitique international et le durcissement de la compétition stratégique qui se décline de manière accélérée et de plus en plus désinhibée sur le plan économique font apparaître un lien direct, assumé et même encouragé chez nos plus féroces compétiteurs entre sécurité nationale et sécurité économique. Ce « nouveau paradigme » s'impose à nous ; il est appelé à refaçonner les équilibres internationaux par la remise en cause des grands principes en vigueur depuis l'Après-Deuxième Guerre mondiale. L'ordolibéralisme (*Ordoliberalismus*) est inexorablement concurrencé par l'interventionnisme étatique.

Le « nationalisme économique » est une réalité. Tout partenaire est aussi un concurrent économique, fût-il un allié, et peut, selon ses intérêts, agir ponctuellement de manière hostile contre notre propre écosystème. De fait, le niveau actuel d'interdépendance économique à l'échelle du globe ne contraint que partiellement les démarches « nationales » des grandes puissances et de nombreux autres acteurs régionaux en voie d'affirmation, visant à la consolidation des souverainetés dans les filières stratégiques en particulier.

Le marché européen est aussi une arène de compétition. Bien que l'on en encense les vertus depuis des décennies, ce marché est de facto une arène convoitée, pénétrée voire exploitée par des acteurs extra-européens (la Chine et les Etats-Unis sont de plus en plus agressifs), mais aussi « manipulée » en interne entre États membres concurrents selon des logiques nationales.

Un contexte

Il s'agit d'appréhender de la manière la plus précise et la plus objective qui soit le **contexte intérieur** français d'une part, i.e., les forces et faiblesses en matière économique de l'entreprise France, et le **contexte extérieur** d'autre part, i.e., l'environnement régional et international dans lequel la France évolue, dans toutes ses configurations et modalités.

Pour cela, l'intelligence économique est un savoir-faire indispensable, d'autant que l'analyse du contexte, par essence dynamique, est un exercice permanent qui repose en outre sur des capacités d'anticipation à développer pour assurer la pertinence de la stratégie nationale conduite.

Nous renvoyons ici le lecteur au contenu de l'étude où sont exposés les éléments utiles à la juste compréhension du contexte.

Une vision et un état final recherché

Une vision doit répondre à la question suivante : en matière de sécurité économique, indissociable, nous l'avons vu, de la sécurité nationale, que veut la France ?

Y répondre, c'est tout d'abord se poser la question de la définition d'une politique économique, a minima d'une politique industrielle, globale ou à multiples échelles sectorielles. Seule cette étape permettra d'arrêter un état final recherché (EFR), à comprendre non pas comme un but figé ou un point à atteindre, mais comme un référentiel dynamique. Que veut-on pour l'économie française à moyen et long terme ? Autour de quels piliers et compétences, et selon quelles priorités envisage-t-on de la structurer (le tout, évidemment, dans un contexte international mouvant dont nous

comprenons toutefois aujourd'hui les grandes orientations et tendances déjà dessinées) ? La réindustrialisation est à l'ordre du jour : quels sont nos objectifs concrets et à quel horizon ? Quels sont les secteurs ou filières prioritaires à « maîtriser » dans une logique de souveraineté, pour atteindre quel but ? Quelles sont les « batailles d'arrière-garde » à abandonner ?

Telles sont quelques-unes des questions qu'il nous paraît indispensable de se poser et, surtout, auxquelles il convient d'apporter des réponses argumentées, concrètes et réalistes sous la forme d'objectifs et de plans d'action.

Des intérêts

La définition des intérêts, et leur catégorisation en fonction de leur caractère plus ou moins vital, majeur, prioritaire ou urgent, est un exercice d'autant plus difficile qu'il requiert une forme d'introspection. Il présuppose en effet l'examen attentif et objectif de nos ambitions comme de nos capacités, et est indissociable d'une réflexion plus vaste et plus profonde sur la manière dont l'« équipe France », dans le domaine qui nous intéresse, voit sa place, son rôle et son action. A minima, il doit permettre de se concentrer sur des points clés qui constituent l'armature de la puissance économique française, ses piliers, qui permettront de définir des objectifs réalistes au service de la vision précédemment arrêtée.

Une remarque s'impose ici. L'école de la déconstruction n'hésite pas à dénoncer la notion d'intérêt national au motif qu'elle ne serait jamais qu'une abstraction inepte et fallacieuse fleurant le nationalisme réactionnaire. La réalité de ce monde, pourtant, pour celui qui accepte de voir ce qu'il voit, et, comme le conseillait Raymond Aron, se méfie des abstractions, est tout le contraire : l'intérêt national est au cœur de toutes les politiques, quelle que soit leur nature, pensées et conduites par les puissances qui comptent et qui agissent. Assimiler intérêt national à nationalisme étriqué, là est la tromperie. Car un intérêt national peut très bien revêtir une dimension d'ouverture multinationale ou internationale, ou appeler à la coopération mutuelle, etc. Là encore, le concept de souveraineté constitue la clé de lecture ; à partir de là seront déclinés des composants qui se combineront ensuite pour former ces intérêts, lesquels s'articulent avec les concepts de souveraineté, d'indépendance et d'autonomie stratégique.

Il nous paraît donc utile d'émettre, à titre d'exemple, la proposition suivante : *« afin de garantir un modèle socioéconomique de développement et de prospérité viable dans la durée (but général ou EFR dynamique), la France doit impérativement assurer sa souveraineté économique (a minima, le contrôle des filières stratégiques et son autonomie d'action et de décision) »*. Sont avancés comme exemples les intérêts suivants :

Intérêt/grand objectif n°1 : Maîtriser les chaînes d'approvisionnement en minéraux et matériaux critiques/stratégiques.

Intérêt/grand objectif n°2 : Disposer d'un niveau de maturité technologique dans les filières d'avenir qui permette de concurrencer des modèles alternatifs.

Intérêt/grand objectif n°3 : S'appuyer sur une économie « réindustrialisée », selon des priorités et des horizons à définir précisément (secteurs, filières, etc.), qui confère à la France un poids incontournable dans les secteurs productifs à l'échelle régionale et internationale.

Intérêt/grand objectif n°4 : Bénéficier d'une autonomie énergétique qui immunise la France contre les manœuvres hostiles étrangères (création de dépendances, chantage, etc.).

Des objectifs

Ceux-ci découlent des intérêts précédemment définis car leur atteinte les sert. Ils n'ont d'ailleurs pas à se limiter au strict champ économique, mais doivent aussi intégrer des paramètres politiques, diplomatiques, normatifs, juridiques, etc.

Ces objectifs seront ensuite déclinés, pour chacun d'eux, sous la forme de tâches ou d'actions à accomplir, et donc éventuellement assortis de plans d'action. Un seul intérêt peut générer de multiples objectifs. Nous offrons ci-dessous les exemples suivants :

(Référence n°1) :

- Établir des accords bilatéraux (multilatéraux au besoin, sous garantie) avec des partenaires disposant des ressources recherchées afin de garantir un approvisionnement optimal en matière de minéraux et matériaux critiques/stratégiques ;
- Soutenir les projets nationaux d'exploitation minière en fonction de besoins prioritaires.

(Référence n°2) :

- Encourager les investissements extérieurs (contrôlés) dans les secteurs de pointe ;
- Investir en R&D dans le secteur des nouvelles énergies (petits réacteurs modulaires (PRM), hydrogène, hydroélectricité, batteries de nouvelle génération, etc.) ;
- Investir en R&D dans le secteur du numérique (IA, technologies de type *cloud*, etc.) ;
- Exercer une influence au sein de l'UE pour assouplir certaines normes (cas actuel de la CRSD) afin de promouvoir des politiques d'innovation et de prise de risques.

(Référence n°4) :

- Entraver les démarches hostiles de certains concurrents par des mesures de toute nature (influence, désinformation, sanctions, contentieux juridique, etc.) ;
- Accélérer la redynamisation de la filière nucléaire.

Des menaces

Tous les capteurs, mobilisés par la « science » de l'intelligence économique, ont pour mission constante d'évaluer et de comprendre l'état de la menace, dans ses dimensions explicite ou implicite, avérée ou potentielle, sur toute la gamme des domaines d'action. Ces menaces doivent être priorisées afin d'assurer une cohérence entre leur prise en compte, l'atteinte de nos objectifs et le service de nos intérêts.

Nous renvoyons le lecteur au contenu de l'étude qui met en valeur la diversité et la dynamique de la menace, ainsi que des risques associés.

Des opportunités

Des opportunités peuvent être identifiées et doivent aussi être recherchées voire provoquées. Elles sont le fruit possible des actions combinées au service des objectifs rapportés à la menace. Les propositions suivantes sont autant d'exemples :

Opportunité n°1 : L'émergence d'une vulnérabilité étrangère (savoir-faire technique déficient, besoin d'investissements) à exploiter car alignée sur un besoin national.

Opportunité n°2 : Une situation nouvellement créée par une interaction avec un partenaire (un accord conclu dans un secteur précis peut permettre d'avoir accès à des filières de sous-traitance par exemple).

Opportunité n°3 : Une réorientation stratégique de la part d'un partenaire-concurrent sous pression excessive de la compétition systémique sino-américaine (ex : volonté de diversification des partenariats de nature économique à des fins de confortement de sa souveraineté, etc.).

Des voies (méthodes) et moyens

Il s'agit de traiter du « comment » ou encore de la doctrine. La méthode que nous préconisons est celle de l'approche proactive plutôt que celle d'une logique défense-attaque assez mal adaptée au contexte économique. L'approche proactive inclut une dimension d'influence explicite, un point clé dans le contexte actuel, et encourage à l'initiative et à la prise de risques.

En toute logique, la gamme des moyens employés doit refléter celle des menaces identifiées. La France dispose d'atouts et de capacités dans tous ces domaines, qu'il lui faut activer avec cohérence. Dans une logique proactive, elle pourrait développer et intensifier des actions de type :

Renseignement : recherche de l'information, captation de données (y compris au sein d'entreprises étrangères invitées), débauchage, entrave, mais aussi exploitation et diffusion au profit du tissu industriel français par exemple.

Information : intelligence économique, attaque réputationnelle ou instrumentalisation d'acteurs non gouvernementaux (ONG), etc.

Finances : investissements ciblés, prises de participation, etc.

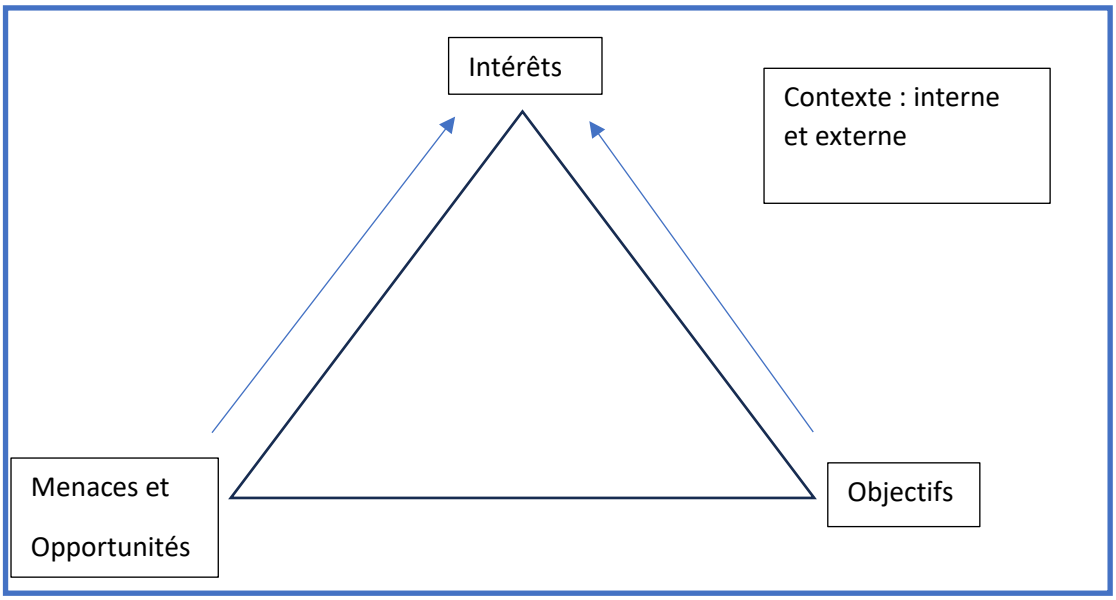
Juridique et règlementaire : activation de dispositifs de protection ou de coercition, recours au contentieux, etc.

Diplomatique : compréhension des marchés locaux, aide à l'implantation, promotion de nos capacités et savoir-faire, etc.

Démarche proactive : conquête de nouveaux marchés, pression via le contrôle des exportations, etc.

Seront donc combinées des actions de protection, de façonnement, de conquête ou encore d'adaptation par le recours à toute la palette des moyens existants et mis en œuvre par nos concurrents. Cette approche proactive présente également selon nous l'avantage d'éviter l'écueil de la surenchère protectionniste (la France, comme nous l'avons vu, dispose d'un arsenal bien plus étoffé que celui de nombre de ses concurrents) qui incite à l'escalade des tensions d'une part, et instille un état d'esprit défensif inhibiteur d'autre part.

Le modèle du « triangle stratégique »



Ce canevas étant posé, il importe de le faire vivre. Or, pour cela, c'est à une véritable réorganisation de l'État, en lien avec les acteurs publics et privés, que l'on appelle. Le constat est unanime : il y a trop d'acteurs, trop de référents, les capacités et les responsabilités sont dispersées, voire diluées, et les acteurs économiques essentiels, les grands groupes mais surtout les ETI-PME-TPE, peinent à faire face à cette complexité[267].

32 - Des recommandations concourantes sous forme de lignes d'opérations (LO)

L'étude menée au cours des six derniers mois a permis d'identifier un certain nombre de problématiques qu'il nous semble indispensable de prendre en compte pour orienter et renforcer la politique française en matière de sécurité économique. Plutôt qu'une liste sans fin d'actions de toute nature à mener, nous proposons une grille de lecture thématique qui offre une architecture à la fois conceptuelle et pratique. Pour chaque thématique, quelques pistes d'action sont proposées.

LO 1 : S'organiser[268]

Une stratégie suppose une organisation. Nous proposons donc que soit menée une réflexion sur la conception et la mise sur pied d'une structure nationale qui englobe toutes les fonctions associées à la sécurité économique, dont l'IE, qui soit décisionnaire, adaptée aux échelons central et territorial, et qui puisse ainsi définir, orienter, conduire, décider et évaluer l'ensemble de l'action de l'équipe France.

Les pistes suivantes, sans intention d'exhaustivité, et sans ordre de priorité, sont évoquées comme autant de possibilités à étudier en gardant à l'esprit que la structure en question doit être dotée de prérogatives décisionnelles :

Élysée : en s'appuyant sur la structure de coordination qu'est la CNR-LT, mais en la conservant distincte, établir un état-major (EM) placé sous l'autorité directe de la Présidence, qui engerbe l'ensemble des fonctions et des dispositifs, centraux et territoriaux, associés à la sécurité économique. Un tel EM serait composé de directions couvrant les principaux domaines suivants : renseignement-anticipation-influence ; opérations (court et moyen terme) et planification (moyen et long terme) ; coordination-liaison (interne France et international) ; évaluation-retour d'expérience-exploitation ; communication. Cet EM structurerait la politique nationale, conduirait la stratégie, selon l'approche proactive évoquée précédemment, coordonnerait, orienterait et évaluerait l'ensemble des acteurs et dispositifs et, surtout, garantirait la cohérence d'ensemble en tant qu'arbitre et décideur, sous l'égide de la présidence ;

Premier ministre (PM) : l'état-major décrit supra pourrait être placé sous l'autorité du PM, selon une approche favorisant la dimension interministérielle de la stratégie. Dans ce cas, il pourrait soit être rattaché au Cabinet du PM, soit constituer une entité autonome ;

[267] Propos tenus dans le cadre d'entretiens avec certains services, le MEDEF et des entreprises diverses (PME et start-ups).
[268] Annexe 3 – Modèle d'état-major.

Autorité indépendante, administrative (AAI) ou publique (API) : ce modèle est évoqué sans conviction en raison des limites qui sont les siennes en matière de réglementation et surtout de décision, et qui semblent difficilement compatibles avec l'ambition affichée et l'ampleur du domaine à « piloter ».

LO 2 : Connaître, anticiper et influencer

La connaissance

La connaissance (compréhension du contexte, y compris interne, des acteurs concernés et des enjeux) et la maîtrise de l'information et des données sont évidemment indispensables à la conduite d'une stratégie. Deux « instruments » sont nécessaires : le renseignement, activité régalienne de collecte d'information selon des modalités spécifiques, dont l'ingérence, et l'intelligence économique, en son sens de collecte légale à partir de sources ouvertes. Ces deux instruments permettent en outre d'appliquer une politique d'influence, régionale et internationale.

Sur le plan interne, nous recommandons d'établir un « *Observatoire des menaces et des risques économiques* », attaché à l'état-major évoqué supra, qui permettrait d'affiner l'ensemble des données relatives à la situation réelle des entreprises de tout type, et de travailler sur des hypothèses et scénarios de risques ; nous estimons par ailleurs qu'un travail de suivi systémique de certaines ONG est indispensable.

Sur le plan externe, les deux instruments précités joueront leur rôle aux fins recherchées. S'agissant tout particulièrement de l'IE, nous abondons dans le sens du rapport Lienemann qui préconise la mise sur pied d'un écosystème IE plus développé, là aussi coordonné par l'état-major, ce qui impliquera d'accroître substantiellement le niveau d'interaction entre les sphères publiques et privées, entre le monde de l'administration (incluant les SR) et celui des entreprises.

L'anticipation

Cet exercice est difficile et n'est que mal maîtrisé par l'administration en général, souvent faute de temps et de ressources, à l'exception du MINARM en particulier. Nous recommandons d'utiliser le Haut-Commissariat à la stratégie et au plan pour établir une feuille de route dans ce domaine et, par exemple, mutualiser les travaux des directions d'anticipation stratégique, ou équivalents, des différents ministères ou autres entités, mais aussi des entreprises concernées et des organismes compétents en la matière (*Futuribles* par exemple, dont la maîtrise méthodologique est précieuse).

L'anticipation est par ailleurs une fonction essentielle du renseignement. Sur le plan économique, un travail en coordination étroite avec l'Observatoire évoqué, et les directions d'anticipation de l'écosystème, nous paraît indispensable.

L'influence

Désormais sixième fonction stratégique, l'influence n'est heureusement plus un gros mot en France. Elle n'est pas pour autant une pratique « naturelle ». Elle l'est d'autant moins qu'une stratégie d'influence dans le domaine qui nous concerne doit découler d'une « grande stratégie » de sécurité économique qui identifie les objectifs à atteindre et coordonne les différentes actions à mener pour y parvenir. Sans ce prérequis, lui-même dynamique, l'influence est réduite à sa portion congrue, c'est-à-dire, au mieux, à une juxtaposition de démarches ponctuelles plus ou moins hasardeuses.

L'influence consiste avant tout à façonner l'environnement dans le sens de nos intérêts. L'enjeu normatif nous paraît être au cœur, aujourd'hui et demain, de cette entreprise. À nous d'identifier les domaines d'avenir qui constituent pour nous une priorité au regard de notre grand objectif de souveraineté, sans oublier qu'être influent requiert d'être crédible, et de faire en sorte que les standards qui les régiront soient compatibles avec nos ambitions et nos intérêts. C'est pourquoi nous

pensons qu'en amont de tout plan d'action en ce domaine, pour éviter de se disperser ou de se satisfaire de discours ou autres déclarations incantatoires, il sera nécessaire de clairement définir le périmètre concerné ainsi que les cibles à privilégier.

LO 3 : Former et sensibiliser (entreprises, élus, centres de recherche, universités, etc.)

Sensibilisation et formation sont à l'ordre du jour depuis quelques années, comme évoqué à plusieurs reprises dans le contenu de cette étude. Toutefois, les résultats ne sont pas encore à la hauteur des attentes. Trois facteurs peuvent expliquer cette situation. En premier lieu, une menace dynamique qui appelle à des adaptations permanentes. Deuxièmement, un certain retard pris dans l'adoption de mesures de protection et, plus largement, dans l'adaptation des comportements, qui est difficile à combler. Le rattrapage implique des changements profonds, y compris organisationnels (méthodes de travail, etc.) qui ont un coût et s'inscrivent dans le temps long. Enfin, sur le plan culturel, que l'on approche le problème sous l'angle du « patriotisme économique » ou de la prise en compte de la conflictualité, la France n'est toujours pas au rendez-vous. Nous recommandons donc :

D'adapter le message à la réalité vécue par les entreprises, en particulier les ETI, PME et TPE, et à leurs contraintes, souvent minorées ou mal appréhendées depuis Paris. Il faut, pour cela, incarner et opérationnaliser le message[269] car ces entreprises répondent avant tout à une logique, celle des gains immédiats. Si les mesures recommandées alourdissent les dispositifs normatifs existants jugés d'ores et déjà étouffants[270], ces acteurs ne répondront pas favorablement aux démarches préconisées. Dans les faits, il faut démontrer que les entreprises ont un intérêt concret et immédiat à la mise en œuvre de certaines mesures, et adapter celles-ci à leurs spécificités, en évitant les généralisations abusives. Dans le domaine de la cybersécurité par exemple, les acteurs rencontrés constatent que des programmes trop ambitieux s'imposant à tous sans discrimination sont contournés au quotidien par une partie du personnel.

D'inciter fortement à la mise en place de cursus de formation à la sécurité économique dans toutes les écoles et universités des filières scientifiques, technologiques, techniques, commerciales, etc. En cela, les préconisations du rapport Plassard nous paraissent très insuffisantes car limitées aux filières de la BITD. Des cours de géopolitique sont indispensables, en guise d'introduction, dans toutes les filières. Mais il convient de les compléter par des modules dédiés à la sécurité économique, incluant l'IE, afin de permettre aux étudiants, à travers des cas concrets, de comprendre les véritables enjeux, menaces et risques qui caractérisent leur environnement[271].

D'introduire dans tous les cursus du secondaire des modules d'initiation aux principes fondamentaux de l'économie et, surtout, d'apprentissage de la gestion au quotidien d'un budget, etc. Nous pensons que par ce biais nous éveillerons les futurs adultes-citoyens à la réalité de la vie économique.

D'intensifier l'effort fourni au profit des élus locaux. Les programmes de sensibilisation aux risques numériques dans les collectivités territoriales existent depuis plusieurs années. Leur systématisation nous paraît indispensable (tout élu doit recevoir, dès son élection, une formation adaptée), de même que la justification des prestations non réalisées.

[269] Les témoignages de start-ups et du MEDEF convergent en ce sens.
[270] Selon les entreprises consultées, très peu d'employés, de manière générale, prennent connaissance de la documentation diffusée.
[271] Cité par le MEDEF, le cas de l'École supérieure des technologies et des affaires (ESTA), Belfort, voir p. 50.

D'opérationnaliser les actions de formation dans une logique de préparation d'un vivier de recrutement. Un des objectifs pourrait ainsi être d'attirer à terme dans les sphères publiques des profils économiques compétents et d'instaurer des parcours dynamiques, moins sclérosés qu'aujourd'hui, en facilitant les allers-retours entre le monde de l'entreprise, l'administration et les services de renseignement par exemple.

LO 4 : S'adapter et innover

Face à la dynamique du phénomène de l'ingérence, une approche proactive et innovante est souhaitable. En ce sens, plusieurs sujets méritent une attention renouvelée :

Lawfare *:* encourager le développement d'une filière française de l'audit et de la conformité.

Cyber : faciliter le développement des compétences nationales et planifier, à moyen terme, le déploiement d'un écosystème numérique souverain, véritablement, dans toutes les filières critiques (BITD et entreprises stratégiques). Certes, cela requiert des investissements substantiels, mais l'évolution des rapports de force et des équilibres géopolitiques, sauf à se voiler la face, ne nous laissent pas le choix.

Potentiel humain : il s'agit, d'une part, de la lutte contre le débauchage. Celle-ci doit être étendue bien au-delà des dispositions de l'article 42 de la LPM pour couvrir également tout le personnel civil (personnel de direction d'entreprise, chercheur retraité, etc.) contre le débauchage duquel nos instruments juridiques sont tout simplement inopérants ; d'autre part, d'imposer des critères de recrutement au sein de l'administration, et notamment au sein de tous les services de renseignement, qui soient favorables à des profils économiques, car ceux-ci apporteront compétence et crédibilité à notre écosystème.

Juridique : en sus des pistes d'action précédemment évoquées, il nous semble judicieux de faire évoluer nos dispositifs juridiques pour introduire dans le code des douanes à la fois la notion d'ingérence, en tant que crime ou délit, et la possibilité du contrôle des biens intangibles en intra-Union (transferts immatériels).

LO 5 : Évaluer et sanctionner

L'évaluation de la pertinence et de l'efficacité des dispositifs en place et des actions menées est indispensable à la manœuvre stratégique que nous préconisons. Depuis des années, les cas concrets se sont accumulés et des décisions, d'agir ou de ne pas agir, ont été prises. Il faut aujourd'hui formaliser un processus dit de retour d'expérience qui puisse enrichir une base de données nationale, nourrir une réflexion partagée et éclairer les choix futurs. Ce processus, itératif et permanent, doit être piloté par l'état-major évoqué supra.

D'ores et déjà, nous pouvons affirmer que la problématique de la sanction sera mise en relief par le RETEX. En effet, au sein de l'administration, et en dehors, existe un consensus sur l'inadaptation des dispositifs de sanction, au périmètre et à l'impact trop limités. Ainsi, les infractions commises, par exemple dans les laboratoires et centres de recherche (domaine de la PPST), débouchent rarement, voire jamais, sur des sanctions administratives à l'encontre des agents ou professeurs responsables, sans même parler du pénal. Par ailleurs, au niveau national, bien que les dispositifs de sanction dans le cadre de la loi Sapin 2 soient complets et crédibles, aucune sanction n'est prévue à l'encontre des acteurs publics tombant sous le coup d'une procédure de l'AFA. Enfin, la loi de « blocage » de 1968 prévoit des barèmes d'amendes insignifiants et nullement dissuasifs (le rapport Plassard souligne ce point et appelle à une augmentation des barèmes).

Il nous paraît donc urgent de systématiser le principe de la sanction, administrative, pénale ou financière, d'en élargir le périmètre à l'ensemble des acteurs, publics et privés, et de relever les seuils existants de manière sensible par souci de crédibilité interne, mais aussi externe.

LO 6 : Faire savoir au « grand public »

Il n'y aura pas d'équipe France sans objectif commun. Or, il n'y a pas d'objectif commun sans partage des informations et des faits. En l'espèce, les avis sont unanimes : l'indifférence du public et le déficit d'attention culturel constatés en France constituent un handicap pour mener à bien une mobilisation de tous les acteurs concernés. Les campagnes internes de sensibilisation et de formation, comme vu supra, portent certains fruits, mais ne suffisent pas, à l'évidence. Nous recommandons donc de franchir le pas et d'oser mettre en œuvre une politique nationale de communication résolument offensive sur la thématique générale de la sécurité économique. Cela impliquerait :

Une synergie communicationnelle entre l'État et les acteurs du monde de l'entreprise qui pourrait se traduire par des campagnes d'information régulières à l'échelle nationale.

Une ouverture des principaux médias à ces questions, en lien avec les experts du monde académique.

Une communication plus ouverte et plus soutenue de la part des autorités elles-mêmes, y compris des responsables des services de renseignement, à l'instar des interventions récentes de la directrice de la DGSI.

Là encore, il s'agirait d'être très concret, c'est-à-dire d'accepter de diffuser des informations correspondant à des dossiers réels qui soient illustratives des actions subies, et de leur impact en matière de coût et d'emploi pour la société en général. La mise en ligne de bulletins d'information par la DGSI et la DRSD notamment s'inscrit certes dans cette démarche, mais le grand public n'y est pas encore sensibilisé. Les quelques « coups de sonde » effectués par l'auteur auprès du grand public ces derniers mois sont très révélateurs : la situation est méconnue et mal comprise ; expliquée et illustrée par des exemples concrets, elle touche et convainc aisément.

L’auteur

Didier Gros, chercheur associé de la Chaire Renseignement de Sciences Po Aix et de la Fondation pour la Recherche Stratégique (FRS), est spécialiste des questions militaires et opérationnelles, de la politique de défense américaine et des relations transatlantiques. Il enseigne à Sciences Po Aix dans le cadre du Mastère Spécialisé « Renseignement et anticipation des risques et menaces » ainsi qu’à Sciences Po Lyon. Il exerce par ailleurs une activité de conférencier et de consultant en stratégie au sein de DPG Conseil.

Colonel (er) diplômé de Saint-Cyr, il est breveté de l'École de guerre française (2004) et du *National War College* américain (2015). Sa carrière militaire l'a conduit sur plusieurs théâtres d'opérations extérieures — en Afrique (République centrafricaine, Côte d'Ivoire, Tchad), dans les Balkans et en Afghanistan — avant d'occuper un poste de cadre-professeur à l'École de guerre à Paris (2013-2014). Spécialiste des relations franco-américaines, il a été affecté à deux reprises à l'ambassade de France à Washington, D.C. : d'abord comme Attaché adjoint (2006-2009), en charge des dossiers interarmées et renseignement, puis comme Attaché militaire (2015-2018).

De 2018 à 2020, il a été détaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN) en qualité de Sous-directeur Affaires internationales. À ce titre, il a assuré le suivi des crises internationales et coordonné des travaux dans les domaines de la lutte contre le terrorisme (dimension extérieure) et contre les menaces hybrides, tout en conduisant des dialogues stratégiques et des exercices d'anticipation stratégique en lien avec la Coordination nationale du renseignement et de la lutte contre le terrorisme (CNR-LT).

Annexe 1 - Entretiens

Administration centrale

Élysée

Coordination nationale du renseignement-Lutte contre le terrorisme -CNRLT

Premier Ministre

Secrétariat général de la défense et de la sécurité nationale-SGDSN

Direction des Affaires internationales, stratégiques et technologiques – AIST

Protection du patrimoine scientifique et technologique-PPST

Conseiller juridique AIST

Conseiller industrie et numérique du Secrétaire général

Sous-direction Affaires internationales

Ministères

Ministère de l'économie, des finances et de la souveraineté industrielle et numérique-MINEFI

Service de l'information stratégique et de la sécurité économiques-SISSE (MM. Gustave Gauquelin et Jérôme Dupré, magistrat détaché)

Agence française Anti-corruption-AFA (M. Mathieu Kahn, Sous-directeur Acteurs économiques)

Direction nationale du renseignement et des enquêtes douanières-DNRED

Ministère des Armées-MINARM

Direction générale de l'armement-DGA

- Sous-direction de la protection et de la résilience des entreprises (M. Jean-Baptiste Kerveillant, Sous-directeur)
- Sous-direction Intelligence économique (M. Camille Lanet, Sous-directeur)

Institut des hautes études de la défense nationale-IHEDN (IGA (er) Jean Roujansky)

Académie du renseignement-ACADRE (M. Jean François Gayrault, Directeur)

Services de renseignement

CNRLT

Direction générale de la sécurité intérieure-DGSI

DNRED

Direction du renseignement et de la sécurité de la défense-DRSD (via les séminaires)

Administration régionale et territoriale

Préfet délégué à la défense et à la sécurité (PDDS) de la région AURA (M. Antoine Guérin, Préfet)

Pôle SAFE de la région PACA (Mme Magali Jaffard)

Monde de l'entreprise

Mouvement des entreprises de France-MEDEF/Commission pour la souveraineté et la sécurité économiques

PME-Eutelsat

Start-ups

- Nawa Technologies (Mme Magali Jaffard)
- Ternwaves (Mme Julie Duclercq, Présidente-Directrice générale)

Monde académique et experts

IRSEM (Mme Maud Quessard, M. Paul Charon, M. Maxime Audinet)

FRS (Mme Annabelle Livet)

EGE-EPGE (M. Charles Pahlawan, Directeur-adjoint)

Experts renseignement, sécurité économique, intelligence économique, cybersécurité

- Général (2S) Serge Cholley, Chaire renseignement, IEP Aix-en-Provence
- M. Nicolas Moinet, professeur des universités, Poitiers
- M. Nicolas Ravailhe, avocat
- M. Laurent Delhalle, conseiller intelligence économique, Implid, Lyon
- M. Jean-Florian Bacquey-Roullet, BRDev
- M. Frédéric Pierucci, dirigeant d'entreprise

Annexe 2 – Exemples de Communautés du renseignement

Etats-Unis d'Amérique (Intelligence Community – IC)

The IC is Comprised of the Following 18 Elements:

TWO INDEPENDENT AGENCIES

1. The Office of the Director of National Intelligence (ODNI)
2. The Central Intelligence Agency (CIA)

NINE DEPARTMENT OF DEFENSE ELEMENTS

The following elements also receive guidance and oversight from the Under Secretary of Defense for Intelligence and Security (USD I&S)—

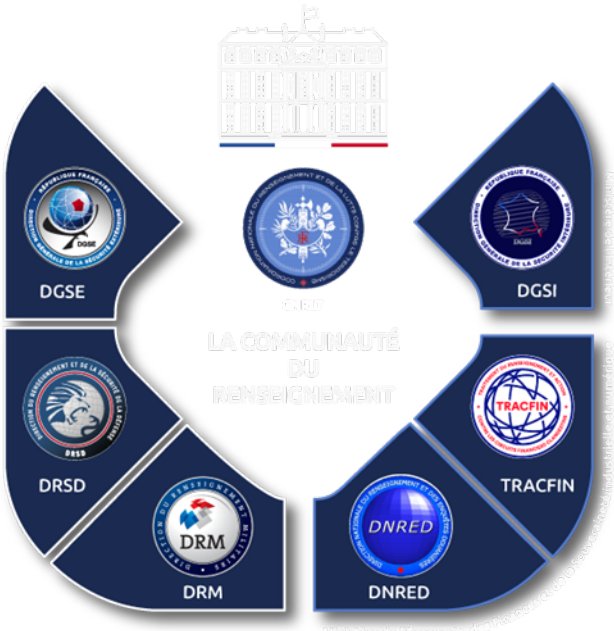
1. The Defense Intelligence Agency (DIA)
2. The National Security Agency (NSA)
3. The National Geospatial-Intelligence Agency (NGA)
4. The National Reconnaissance Office (NRO)
5. U.S. Air Force Intelligence
6. U.S. Navy Intelligence
7. U.S. Army Intelligence
8. U.S. Marine Corps Intelligence
9. U.S. Space Force Intelligence

SEVEN ELEMENTS OF OTHER DEPARTMENTS AND AGENCIES

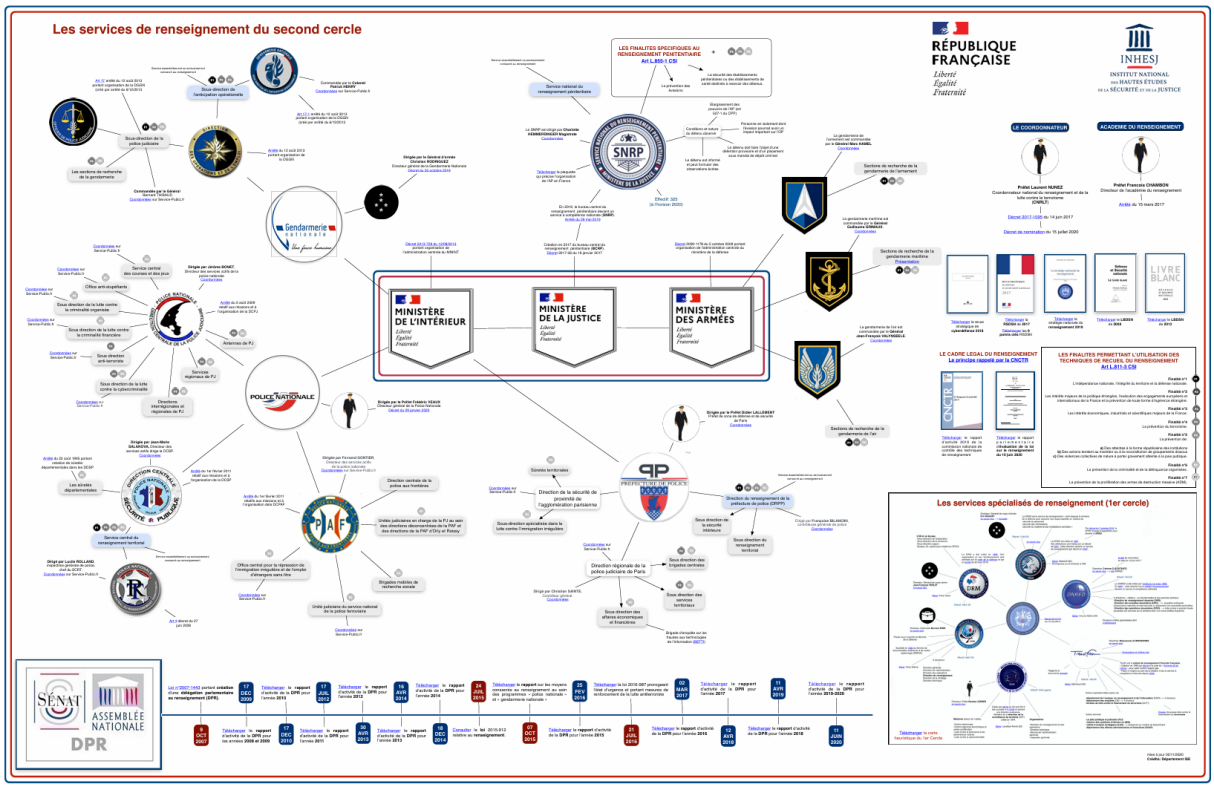
1. The Department of Energy's Office of Intelligence and Counterintelligence
2. The Department of Homeland Security's Office of Intelligence and Analysis and
3. The intelligence and counterintelligence elements of the U.S. Coast Guard
4. The Department of Justice's Federal Bureau of Investigation and
5. The Drug Enforcement Administration's Office of National Security Intelligence
6. The Department of State's Bureau of Intelligence and Research
7. The Department of the Treasury's Office of Intelligence and Analysis

France

Services dits du « premier cercle »



Du « second cercle » : DNRT, DRPP, SDAO, SNRP



Chine

Source : Paul Charon et Jean-Baptiste Jeangène Vilmer, LES OPÉRATIONS D'INFLUENCE CHINOISES, Un moment machiavélien, IRSEM, octobre 2021. Cas du ministère de la Sécurité d'État (MSE), https://drive.google.com/file/d/11XOzrPy3z_1nRsPlKiqktjbgK5aqMClq/view

Annexe 3 – Modèle d'état-major

Autorité hiérarchique : Présidence ou PM