Une étude publiée en juin 2026 par la Chaire Renseignement de Sciences Po Aix, rédigée par le chercheur Didier Gros sous la direction du professeur Walter Bruyère-Ostells, examine la manière dont la France répond aux ingérences économiques étrangères. Elle s'appuie sur des séminaires organisés entre 2023 et 2025 et sur trente-deux entretiens menés au sein de l'administration, des services de renseignement, des entreprises et du milieu académique. Son constat : la France dispose d'un des arsenaux de protection économique les plus complets d'Europe, mais reste, selon l'auteur, sur une posture essentiellement défensive et fragmentée, faute d'une stratégie nationale clairement définie.

L'étude relève un paradoxe. La France subit quotidiennement des ingérences ou tentatives d'ingérence qui affectent son tissu économique, alors même qu'elle est équipée d'un dispositif juridique et réglementaire dense. À la question qu'elle pose – « *que veut la France en matière de souveraineté et de sécurité économiques ?* » – l'auteur estime que la réponse est « *confuse, incertaine voire inexistante* ».

Le document inscrit cette situation dans un contexte international qu'il décrit comme marqué par la fin de la période d'hégémonie américaine ouverte après 1991. Il identifie plusieurs facteurs : l'affirmation de la Chine comme rival systémique, la résurgence russe, l'émergence de puissances régionales et les effets de la mondialisation, notamment la désindustrialisation. Dans ce cadre, l'économie et le droit sont présentés comme des instruments de plus en plus mobilisés à des fins de puissance.

L'auteur défend une définition large de la sécurité économique. Selon lui, celle-ci ne se limite pas à un dispositif de protection : elle est indissociable de la sécurité nationale et doit combiner actions défensives et offensives. Il rappelle que les États-Unis et la Chine retiennent cette approche ; Washington affirmant que « *la sécurité économique est la sécurité nationale* », Pékin ayant formalisé en 2014 un concept de « *sécurité nationale globale* ». L'Union européenne, elle, privilégie une lecture économique fondée sur la gestion du risque, approche que l'ancien président de la BCE Mario Draghi a critiquée pour son manque de coordination.

La nature et les acteurs de la menace

L'étude propose une typologie des menaces : capitalistique, humaine, physique, technique (dont cyber), juridique, réputationnelle et logistique. Elle souligne la difficulté à distinguer l'influence, considérée comme légitime, de l'ingérence, caractérisée par l'illégalité. Les données citées de la DGSI indiquent que, sur environ 2000 alertes annuelles, 10 % correspondent à des ingérences avérées et 90 % à des situations de vulnérabilité, souvent liées à des difficultés financières.

Les États-Unis et la Chine représenteraient à eux deux les deux tiers des actions hostiles recensées. La menace capitalistique (prises de participation et offres d'achat hostiles) reste la plus fréquente.

Concernant les États-Unis, l'étude met en avant la cohérence de leur appareil de sécurité et l'usage du droit à portée extraterritoriale (dispositifs FCPA, ITAR, *Cloud Act*) ainsi que le contrôle des transactions en dollars. Elle cite les cas d'Alstom Power et de BNP Paribas comme

exemples de sanctions ayant conduit à des transferts de compétences ou à une mise sous contrôle d'entreprises françaises.

La Chine est décrite comme agissant « *en miroir* » des États-Unis, avec une intégration civilo-militaire, une loi de 2017 mobilisant ses ressortissants pour la collecte de renseignement, l'usage de ses liquidités et la captation de savoir-faire, illustrée par le cas Ligeance Aerospace. L'auteur mentionne aussi les récentes restrictions chinoises sur les terres rares.

L'étude accorde une place particulière aux partenaires européens, dont l'Allemagne, décrite comme menant une concurrence de plus en plus directe : captation de fonds européens, action sur la filière nucléaire française via des fondations et des ONG, investissements dans le spatial. Le cas de la *start-up* Ternwaves, visée devant l'office américain des brevets à l'initiative d'acteurs allemands, est cité comme exemple. Les pays du Proche et Moyen-Orient (pétromonarchies, Israël, Turquie) sont présentés comme des concurrents en affirmation. La Russie, en revanche, est jugée secondaire sur le plan économique, sa menace relevant davantage de la nuisance ciblée.

Les cas Eutelsat et Exaion sont analysés comme des illustrations du dilemme entre attractivité et souveraineté : comment attirer des capitaux étrangers sans exposer des actifs stratégiques.

Les dispositifs existants et leurs limites

L'étude retrace une prise de conscience qu'elle qualifie de tardive. Malgré le rapport Martre de 1994 et le rapport Carayon de 2003, la France n'a institué une politique publique de sécurité économique qu'en 2019, par décret. Depuis, l'auteur constate une mobilisation réelle : réorganisation de la communauté du renseignement, création de structures dédiées à la DGSI, la DGSE, la DRSD, la DNRED, au SISSE, au SGDSN et à la DGA. L'arsenal comprend le contrôle des investissements étrangers en France (CIEF), la loi de blocage de 1968, la loi Sapin II, le Parquet national financier et l'Agence française anticorruption. Les entreprises, via le MEDEF et le rapport Roux de Bézieux, ainsi que le milieu académique de l'intelligence économique, participent à cette mobilisation.

L'étude relève néanmoins plusieurs limites. Elle pointe une posture jugée trop défensive, susceptible de rigidifier l'écosystème et de favoriser son contournement. Elle souligne une fragmentation institutionnelle, l'absence de chaîne de commandement identifiable et une tension entre l'Élysée et Bercy, en l'absence de politique industrielle définie. Le SISSE, chargé de la protection, n'orienterait pas les services de renseignement. L'auteur note aussi un déficit de culture économique dans l'administration et une faible circulation entre le renseignement et le monde de l'entreprise. Il identifie enfin ce qu'il décrit comme un obstacle culturel, lié à l'absence d'un « ***patriotisme économique*** » assumé.

Sur l'Union européenne, l'étude adopte une position nuancée : elle y voit à la fois un cadre potentiellement utile et une source de contraintes, en raison de sa transparence et de certaines normes jugées pénalisantes pour les entreprises européennes.

Deux champs font l'objet d'un examen approfondi. Le *lawfare* (usage du droit comme arme) : la France dispose d'instruments, mais l'auteur les juge peu dissuasifs faute de sanctions

suffisantes. La cybersécurité : l’étude décrit une dépendance structurelle aux technologies américaines et estime que la souveraineté numérique reste un objectif non atteint, malgré les dispositifs de l’ANSSI comme la certification SecNumCloud, dont l’efficacité fait débat.

Les recommandations

La troisième partie formule des recommandations autour d’une proposition centrale : élaborer une stratégie nationale de souveraineté et de sécurité économiques. L’auteur propose un cadre d’analyse, le « triangle stratégique », reliant intérêts, objectifs et menaces ou opportunités. Il suggère de créer une structure décisionnaire — un état-major placé sous l’autorité de la Présidence ou du Premier ministre — chargée de coordonner l’action aux niveaux central et territorial.

Six axes, présentés comme des « lignes d’opérations », complètent cette proposition : s’organiser autour de l’état-major ; connaître, anticiper et influencer, notamment via un « Observatoire des menaces et des risques économiques » ; former et sensibiliser les entreprises, les élus et le public ; s’adapter et innover, en développant une filière d’audit et un écosystème numérique national ; évaluer et sanctionner, en relevant les seuils de sanction ; et communiquer plus largement auprès du grand public, que l’étude considère comme insuffisamment informé.

L’auteur conclut que la définition d’une stratégie suppose au préalable de clarifier la vision économique et industrielle du pays, ainsi que les intérêts qu’il entend défendre.

View Fullscreen
Aller au contenu PDF