INTERNATIONAL JOURNAL OF RESEARCH IN ECONOMICS AND FINANCE, 2026, Vol. 3, No. 6-2, 168-188. https://doi.org/10.71420/ijref.v3i6-2.336

Le spectre de l'hybridité : de l'intelligence économique à l'espionnage économique dans la compétition géo-économique

The Spectrum of Hybridity: From Economic Intelligence to Economic Espionage in Geoeconomic Competition

Alae-Eddine SANOUSSI
Structure de recherche : Gouvernance de l'Afrique et du Moyen-Orient, Faculté des Sciences Juridiques, Économiques et Sociales, Mohammed 5 Université de Rabat, Maroc.

Résumé. Cet article propose un cadre analytique permettant de qualifier et de comparer les pratiques situées sur le continuum qui relie l'intelligence économique à l'espionnage économique dans la compétition géoéconomique. À partir d'une définition opérationnelle de l'hybridité, il construit une grille à quatre dimensions, informationnelle, juridique, technologique et stratégique, puis traduit chaque dimension en indicateurs gradués selon la typologie blanc, gris, noir. Cette grille qualitative est appliquée à deux configurations documentées par des données publiques, comparées de façon argumentée : l'accès extraterritorial aux données et la captation clandestine de secrets d'affaires. Les résultats montrent que le basculement de la compétition vers la prédation procède par glissements cumulatifs plutôt que par franchissement d'un seuil unique. Ils établissent surtout que la configuration la plus exposée n'est pas nécessairement la plus illégale : la combinaison du droit extraterritorial et de la concentration des infrastructures numériques produit un niveau de risque élevé en restant formellement licite. L'article en déduit des recommandations traçables, reliées aux dimensions de la grille et différenciées par acteur, à destination des entreprises, des décideurs publics et des responsables de l'intelligence économique.

Mots-clés : *Intelligence économique ; Espionnage économique ; Hybridité ; Grille d'analyse ; Typologie blanc gris noir ; Compétition géoéconomique ; Extraterritorialité du droit ; Dépendance numérique ; Secrets d'affaires ; Résilience.*

Abstract. This article proposes an analytical framework for qualifying and comparing practices located along the continuum that links economic intelligence to economic espionage within geoeconomic competition. Starting from an operational definition of hybridity, it builds a four-dimensional grid, covering the informational, legal, technological and strategic dimensions, and translates each dimension into indicators graded according to the white-grey-black typology. This qualitative grid is applied to two configurations documented through public data and compared in an argued manner: extraterritorial access to data and the covert appropriation of trade secrets. The results show that the shift from competition to predation proceeds through cumulative slippages rather than the crossing of a single threshold. They establish, above all, that the most exposed configuration is not necessarily the most unlawful: the combination of extraterritorial law and the concentration of digital infrastructures produces a high level of risk while remaining formally lawful. The article derives traceable recommendations, tied to the grid's dimensions and differentiated by actor, for firms, public decision-makers, and economic intelligence officers.

Keywords: *Economic intelligence; Economic espionage; Hybrid threats; Geoeconomic competition; Economic security; Informational sovereignty; Strategic dependence; Digital infrastructure; Surveillance; Resilience.*

1. Introduction

La compétition géo-économique contemporaine place l'information, la donnée stratégique et la capacité d'anticipation au cœur des rapports de puissance (Csurgai, 2017). Dans cet environnement marqué par l'intensification des rivalités économiques, technologiques et normatives, l'intelligence économique s'impose comme un instrument central de compréhension, de protection et de projection des intérêts des États comme des entreprises. Longtemps présentée comme un ensemble de pratiques licites articulant veille, influence et sécurité informationnelle (Germon, 2013, p. 75), elle évolue désormais dans un espace plus instable, traversé par des logiques de confrontation indirecte, de guerre cognitive, de pression normative et de captation clandestine de ressources informationnelles (Weissmann et al., 2021, p. 124).

C'est dans ce contexte que la notion d'hybridité acquiert une portée analytique particulière. Elle permet de penser les zones grises où se brouillent les frontières entre activités défensives et offensives, entre renseignement légal et espionnage, entre compétition économique et conflictualité stratégique (Schmid & Georget, 2021). L'hybridité ne renvoie pas seulement à la combinaison de moyens hétérogènes ; elle désigne aussi un continuum d'actions dans lequel des instruments juridiques, technologiques, informationnels et parfois clandestins se combinent au service d'objectifs de puissance (GROS & VILBOUX, 2021, p. 18). Dès lors, l'intelligence économique ne peut plus être étudiée uniquement comme une pratique de gouvernance de l'information au service de la performance : elle doit également être interrogée comme un espace de bascule possible vers des formes de prédation informationnelle et d'espionnage économique (Moinet & Bulinge, 2013).

L'intérêt scientifique d'un tel sujet réside précisément dans l'examen de cette ligne de crête. Entre la collecte légitime d'informations ouvertes et l'appropriation illicite de données sensibles, entre la protection des actifs immatériels et l'instrumentalisation offensive des vulnérabilités informationnelles, se déploie un véritable spectre de l'hybridité (Filipec, 2021, p. 23). Ce spectre oblige à dépasser les oppositions binaires classiques pour envisager une gradation des pratiques, des acteurs et des finalités. Il conduit également à replacer l'espionnage économique dans une lecture plus large de la conflictualité contemporaine, où la puissance se mesure autant à la maîtrise des infrastructures numériques, des normes juridiques et des flux informationnels qu'à la détention de ressources matérielles (Gabarre et al., 2021, p. 87).

À partir de cette perspective, cet article entend analyser les relations de continuité, de tension et de rupture entre intelligence économique et espionnage économique dans le cadre de la compétition géo-économique. L'hypothèse directrice est que l'hybridité constitue une grille de lecture particulièrement féconde pour comprendre la porosité croissante entre pratiques de veille, stratégies d'influence, dispositifs de sécurité économique et mécanismes de captation clandestine de l'information. Une telle approche permet non seulement de mieux qualifier les transformations de l'environnement stratégique, mais aussi de réfléchir aux conditions de gouvernance, de résilience et de souveraineté informationnelle des acteurs exposés à ces dynamiques.

L'originalité de cet article tient à la manière dont il articule, au sein d'un même cadre analytique, trois champs généralement traités séparément : l'intelligence économique, l'espionnage

économique et la littérature sur les menaces hybrides. Alors que les travaux antérieurs opposent le plus souvent la veille licite aux pratiques clandestines (Chtouki & Deriouch, 2020; Feige et al., 2024), la présente contribution propose de les inscrire dans un continuum gradué et de mobiliser la notion d'hybridité comme grille de lecture transversale (Weissmann et al., 2021, p. 124). La valeur ajoutée du papier réside ainsi dans le dépassement des oppositions binaires entre légal et illégal, défensif et offensif, civil et militaire, au profit d'une approche intégrative reliant pratiques informationnelles, instruments juridiques extraterritoriaux et dépendances technologiques (Bigo et al., 2019, p. 95).

Les contributions de l'article sont de trois ordres. Sur le plan conceptuel, il propose une définition synthétique et opérationnelle de l'hybridité économique et en précise les dimensions analytiques. Sur le plan théorique, il relie la littérature sur l'intelligence économique (Moinet & Bulinge, 2013) à celle sur la géoéconomie (Csurgai, 2017) et sur les menaces hybrides (Filipec, 2021, p. 23), afin de montrer que l'espionnage économique constitue une dérive inscrite dans le champ même de la compétition géo-économique. Sur le plan opérationnel enfin, il débouche sur des recommandations adressées aux entreprises, aux décideurs publics et aux responsables de l'intelligence économique, en matière de gouvernance de la sécurité économique et de renforcement de la résilience informationnelle.

2. Cadre conceptuel : définition opérationnelle de l'hybridité économique

Cet article s'appuie sur une définition synthétique et opérationnelle de l'hybridité économique qui servira de référence pour l'ensemble de l'article. L'hybridité économique est entendue ici comme la combinaison coordonnée et graduelle de moyens licites, ambigus et illicites, qu'ils soient informationnels, juridiques, technologiques ou cognitifs, mobilisés par des acteurs étatiques ou privés afin d'acquérir, de protéger ou de capter de l'information stratégique dans une logique de puissance, au sein d'une zone grise où la frontière entre compétition légitime et hostilité demeure structurellement indécidable (Weissmann et al., 2021, p. 124; GROS & VILBOUX, 2021, p. 18; Filipec, 2021, p. 23). Cette définition prolonge les approches qui conçoivent la guerre hybride comme un brouillage volontaire des seuils entre paix et conflit (Schmid & Georget, 2021; Tenenbaum & Hartpence, 2015).

Quatre dimensions analytiques sont retenues dans le cadre de cet article. La première, informationnelle, renvoie à la gradation des sources et des méthodes de collecte, depuis la veille ouverte jusqu'à la captation clandestine (Baaziz, 2015, p. 126). La deuxième, juridique, concerne l'usage du droit, notamment extraterritorial, comme levier de puissance (Bigo et al., 2019, p. 95). La troisième, technologique, porte sur les dépendances numériques et l'exploitation des vulnérabilités par l'intelligence artificielle (Nowicka et al., 2024, p. 494). La quatrième, stratégique, désigne la dilution de l'imputabilité par le recours à des proxys et à des organisations écran (Langen et al., 2024, p. 344). Ce sont ces quatre dimensions qui orientent l'analyse développée dans la suite de l'article.

3. Méthodologie de recherche

Cet article construit et applique un cadre analytique destiné à qualifier et à comparer les pratiques situées sur le continuum qui relie l'intelligence économique à l'espionnage économique. La démarche articule trois opérations. La première établit une grille à quatre dimensions, dérivée de

la définition opérationnelle de l'hybridité économique exposée dans la section précédente. La deuxième traduit chaque dimension en indicateurs observables et en une gradation qualitative blanc, gris, noir, de sorte que des situations concrètes puissent être positionnées de manière reproductible. La troisième applique cette grille à deux cas documentés par des données publiques, confrontés afin de qualifier leur degré d'exposition au risque hybride. Le cadre ne prétend pas à une mesure statistique de la fréquence des atteintes, donnée que les acteurs concernés ne divulguent pas. Il fournit un instrument de qualification structuré, traçable et transférable, qui rend explicites les critères de jugement et permet la comparaison entre cas.

Le corpus mobilisé se compose de trois ensembles de sources : la littérature académique sur l'intelligence économique et la sécurité économique (Fontanel, 2016; Moinet & Bulinge, 2013; Goria, 2023) ; la littérature sur les menaces et la guerre hybrides (Weissmann et al., 2021; Filipec, 2021; GROS & VILBOUX, 2021) ; et les sources juridiques et institutionnelles relatives à l'extraterritorialité du droit et à la résilience (Bigo et al., 2019; Velliet, 2023; OECD, 2021, 2023). Les sources ont été sélectionnées selon trois critères : leur pertinence conceptuelle au regard de l'hybridité, leur ancrage dans des travaux fondateurs ou récents (2015–2026), et leur capacité à éclairer le passage du légal à l'illégal.

L'analyse est structurée par une grille à quatre dimensions, dérivée de la définition opérationnelle de l'hybridité économique : la dimension informationnelle (gradation des sources, du blanc au noir), la dimension juridique (le droit comme levier de puissance), la dimension technologique (dépendances numériques et intelligence artificielle) et la dimension stratégique (dilution de l'imputabilité). Chaque dimension constitue à la fois un axe de lecture des pratiques et une catégorie d'exposition au risque. Cette grille fournit le fil conducteur des sections suivantes et sert de matrice pour dériver, en conclusion, des recommandations différenciées par type d'acteur.

L'opérationnalisation repose sur une gradation qualitative à trois niveaux, appliquée à chacune des quatre dimensions, selon la typologie blanc, gris, noir. Le niveau blanc correspond à une pratique ouverte et licite, sans ambiguïté. Le niveau gris désigne une pratique dont la licéité dépend du contexte juridictionnel ou de l'intention, légale dans sa forme mais agressive dans ses effets. Le niveau noir caractérise une pratique clandestine ou prédatrice, contraire au droit ou à l'éthique professionnelle, ou un usage du droit comme levier de puissance au détriment de la réciprocité. La grille ne produit aucun indice chiffré : elle qualifie chaque dimension par un positionnement argumenté, justifié par un fait documenté et une référence, ce qui rend la qualification traçable et réfutable.

Trois critères ont guidé la sélection des configurations analysées : leur documentation par des sources publiques vérifiables, leur représentativité des mécanismes hybrides décrits dans la littérature, et leur capacité à éprouver la grille sur des dimensions distinctes. La validité de l'instrument tient à la transparence de ses règles de codage plutôt qu'à la taille de l'échantillon. Sa transférabilité ouvre la voie à des applications ultérieures sur des corpus élargis ou des données de première main, lorsque celles-ci deviennent accessibles.

a. Le cadre opérationnalisé

La grille repose sur quatre dimensions complémentaires. Chacune est définie par un objet d'observation, traduite en indicateurs concrets, et graduée selon la typologie blanc, gris, noir issue

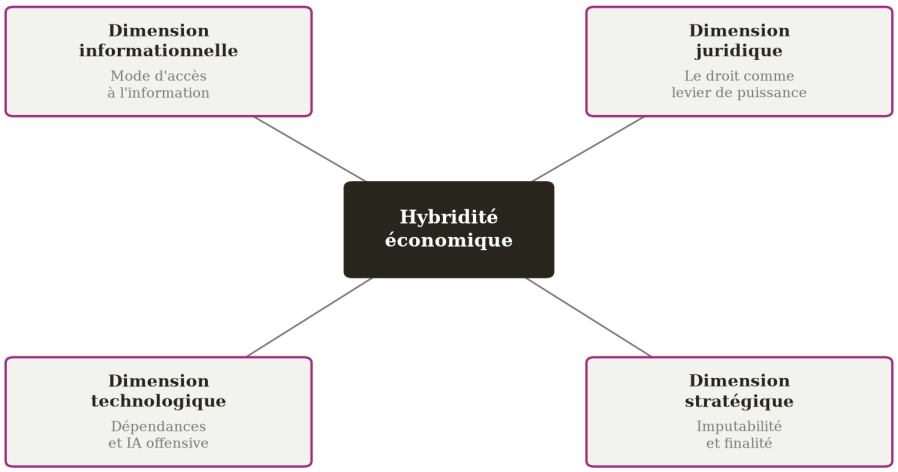
de la doctrine de l'intelligence économique (Baaziz, 2015, p. 126). Le Tableau 1 réunit ces éléments. Il transforme une notion souvent invoquée de manière allusive en un instrument de qualification explicite.

Tableau 1. Matrice des dimensions, indicateurs et gradation blanc, gris, noir.

Dimension	Objet observé	Indicateurs	Blanc (licite)	Gris (ambigu)	Noir (illicite)
Informationnelle	Mode d'accès à l'information	Nature des sources ; méthode de collecte ; consentement de la source	Veille sur sources ouvertes, données publiques	Élicitation, ingénierie sociale, exploitation d'indiscrétions	Intrusion, captation clandestine, vol de secrets d'affaires
Juridique	Usage du droit comme levier	Base légale invoquée ; portée territoriale ; asymétrie de la contrainte	Conformité au droit national, réciprocité	Extraterritorialité, forum shopping normatif	Contournement du droit, instrumentalisation coercitive
Technologique	Dépendance et exploitation des infrastructures	Concentration des fournisseurs ; accès aux données par des tiers ; IA offensive	Infrastructures maîtrisées, réversibilité assurée	Dépendance critique, accès légal extraterritorial aux données	Exploitation de vulnérabilités, exfiltration assistée par IA
Stratégique	Imputabilité et finalité	Attribution de l'action ; recours à des intermédiaires ; objectif de puissance	Action assumée, finalité défensive	Recours à des proxys, finalité ambivalente	Dilution de l'imputabilité, finalité prédatrice

Source : élaboration de l'auteur à partir de Baaziz (2015), Weissmann et al. (2021), Bigo et al. (2019), Nowicka et al. (2024), Langen et al. (2024).

Figure 1. Modèle de la grille à quatre dimensions de l'hybridité économique



Source : Produit par l'auteur

b. Application du cadre : étude de cas comparative de deux configurations documentées

La grille à quatre dimensions est ici appliquée à deux configurations réelles, documentées par des sources publiques vérifiables et choisies pour leur position contrastée sur le continuum. La première, l'accès extraterritorial aux données, relève d'une hybridité légale mais prédatrice : elle mobilise le droit et la dépendance technologique sans franchir le seuil de l'illégalité manifeste. La seconde, la captation clandestine de secrets d'affaires assistée par des moyens cyber, relève du versant ouvertement illicite. Plutôt que d'attribuer une note chiffrée, l'analyse qualifie chaque dimension selon la gradation blanc, gris, noir définie plus haut, et justifie ce positionnement par un fait documenté et une référence. La confrontation des deux cas éclaire ainsi le mécanisme par lequel s'opère le glissement de la veille légitime vers la prédation.

i. Cas A : L'accès extraterritorial aux données : une hybridité légale

Le premier cas combine un levier juridique et une dépendance technologique. Sur la dimension juridique, la section 702 du FISA et le CLOUD Act autorisent les autorités américaines à accéder aux données détenues par les fournisseurs américains, indépendamment du lieu où ces données sont stockées (Bigo et al., 2019, p. 162 ; Velliet, 2023, p. 26). Le nombre estimé de cibles non américaines de la section 702 est passé de 268 590 en 2023 à 349 823 en 2025, ce qui atteste une montée en charge continue du dispositif (ODNI, 2025). Cette dimension se situe au niveau noir, non parce que le droit serait violé, mais parce qu'il est instrumentalisé comme levier de puissance extraterritorial, au détriment de la réciprocité.

Sur la dimension technologique, la concentration du marché amplifie cette exposition : trois fournisseurs réunissent environ 63 % du marché mondial des infrastructures cloud, ce qui crée une dépendance critique difficilement réversible (Synergy Research Group, 2025). Cette dimension se situe au niveau gris : la dépendance résulte de choix de marché licites, mais elle ouvre un accès légal aux données par un tiers étatique. La dimension informationnelle demeure au niveau blanc, car aucune ruse ni intrusion n'est requise : l'accès procède d'un cadre légal et de relations contractuelles. La dimension stratégique se situe au niveau gris, l'action étant assumée mais poursuivant une finalité ambivalente, à la fois sécuritaire et concurrentielle. La configuration est instructive parce qu'elle produit un effet de captation sans recourir à l'illégalité : le droit et la technologie y suffisent (Filipec, 2021, p. 23).

ii. Cas B : La captation clandestine de secrets d'affaires : une hybridité illicite

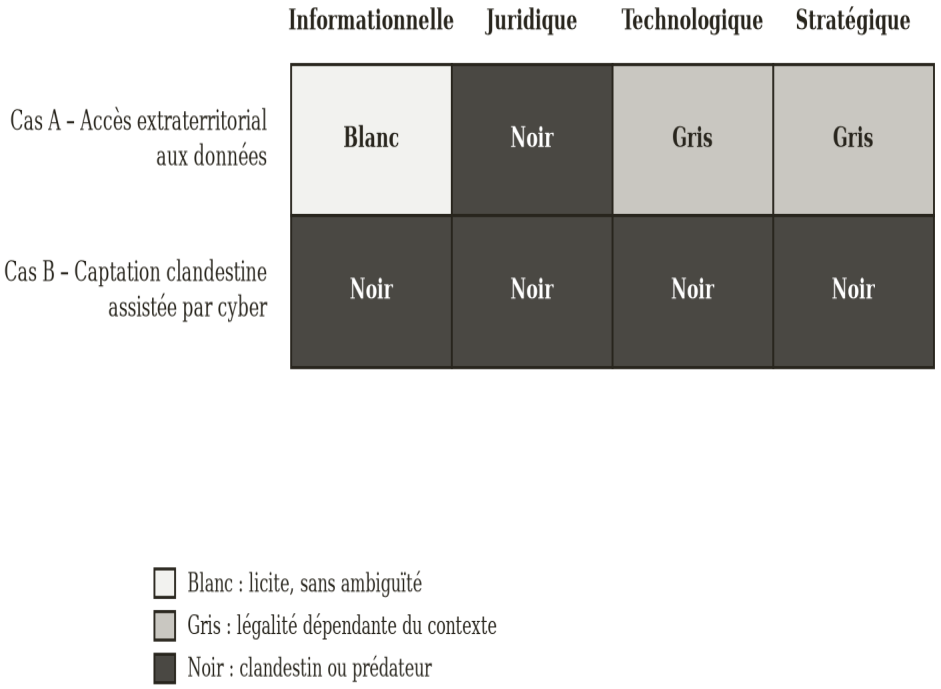
Le second cas se situe à l'autre extrémité du continuum. Les quatre dimensions y atteignent le niveau noir. L'accès à l'information est clandestin, puisqu'il repose sur l'intrusion et la captation dissimulée ; le droit est ouvertement enfreint, la pratique constituant un vol de secrets d'affaires ; la dimension technologique est mobilisée de façon offensive, l'attaque exploitant des vulnérabilités techniques et, de plus en plus, des outils assistés par intelligence artificielle (Nowicka et al., 2024, p. 494) ; la finalité stratégique est prédatrice et l'imputabilité délibérément diluée par le recours à des intermédiaires. Le coût de ces atteintes est documenté : le vol de secrets d'affaires représenterait de 1 à 3 % du PIB des économies avancées, soit un ordre de grandeur de 180 à 540 milliards de dollars par an pour la seule économie américaine (IP Commission, 2017), et près de 60 milliards d'euros de pertes annuelles dans l'Union européenne (Commission européenne, 2019). Ce cas constitue le point de référence du versant noir du continuum, contre lequel se mesure l'ambiguïté du cas précédent.

Tableau 2. Qualification comparée des deux cas sur la grille à quatre dimensions (gradation blanc, gris, noir)

Dimension	Cas A – Accès extraterritorial aux données	Cas B – Captation clandestine assistée par cyber
Informationnelle	Blanc – accès légal et contractuel, sans ruse	Noir – intrusion et captation clandestine
Juridique	Noir – droit instrumentalisé (FISA 702, CLOUD Act)	Noir – violation du droit (vol de secrets)
Technologique	Gris – dépendance critique au cloud concentré	Noir – exploitation offensive de vulnérabilités
Stratégique	Gris – action assumée, finalité ambivalente	Noir – imputabilité diluée, finalité prédatrice

Source : analyse de l'auteur ; données : ODNI (2025), Synergy Research Group (2025), IP Commission (2017), Commission européenne (2019).

Figure 2. Profil qualitatif des deux cas sur les quatre dimensions (gradation blanc, gris, noir)



Source : élaboration de l'auteur.

iii. Lecture transversale

La confrontation des deux cas met en évidence le caractère graduel du basculement décrit par la littérature sur l'hybridité (Filipec, 2021, p. 23). La frontière entre compétition légitime et prédation ne se franchit pas en un seuil unique, mais par accumulation de glissements sur des dimensions distinctes. Le cas A est le plus instructif, car il produit un effet de captation tout en restant largement

dans le champ du licite : l'hybridité économique se loge précisément dans cet interstice où des instruments légaux produisent des effets équivalents à ceux de la prédation (Weissmann et al., 2021, p. 124). Le cas B, ouvertement illicite, fixe le terme noir du continuum et donne sa mesure au glissement observé dans le premier cas. Cette lecture comparée confirme l'hypothèse centrale de l'article : c'est moins la légalité formelle d'une pratique que la combinaison de ses dimensions qui détermine son degré d'hybridité.

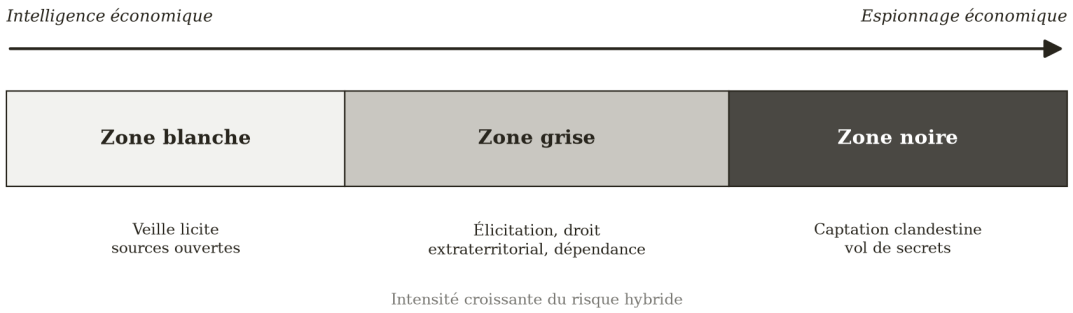
4. Le spectre de l'hybridité : clarification du concept

Pour appréhender la complexité de cette notion, il est nécessaire de déconstruire la distinction traditionnelle qui tend à isoler l'intelligence économique, perçue comme un levier de compétitivité légitime, des procédés illicites inhérents à l'espionnage industriel (Chtouki & Deriouch, 2020; Ocqueteau, 2012, p. 12). Cette frontière, souvent ténue, nécessite une analyse approfondie des cadres juridiques et éthiques qui, dans la pratique, peinent à réguler des méthodes en constante mutation technologique (Razinkina et al., 2022 ; Feige et al., 2024). En effet, si l'intelligence économique se définit classiquement par des pratiques de veille et de protection, elle s'inscrit aujourd'hui dans un continuum où les activités de renseignement et les tactiques d'influence se rejoignent pour servir des objectifs de souveraineté technologique (Goria, 2023, p. 78; Urtmelidze, 2025, p. 2). Cette dynamique est exacerbée par la digitalisation et l'usage accru de l'intelligence artificielle, qui transforment les méthodes de surveillance et d'analyse en des outils capables d'exploiter les vulnérabilités informationnelles en temps réel (Vitanovski & Taneski, 2025a, 2025b). Cette interconnexion généralisée rend la distinction entre les tactiques non militaires et les agressions directes de plus en plus difficile à établir, transformant ainsi les champs de bataille immatériels en espaces où la ruse devient une composante intrinsèque des stratégies de puissance (Georgelin & Holeindre, 2021, p. 95; Kovalchuk, 2025). Cette recomposition stratégique, marquée par une diffusion horizontale des capacités numériques, place les acteurs étatiques et privés face à des menaces hybrides qui exploitent la porosité entre le civil et le militaire (Hamel, 2025). Cette hybridation des menaces se caractérise par une utilisation synergique de cyberopérations, de désinformation et de coercition économique, visant à fragiliser la confiance institutionnelle et la stabilité structurelle des économies modernes (Mazur, 2025). Cette dilution de la responsabilité, souvent opérée par le recours à des organisations écran ou des proxys, complexifie singulièrement l'imputabilité des actions hostiles et entrave les mécanismes de riposte conventionnels (Langen et al., 2024, p. 344). Face à cette complexité, la définition du concept demeure toutefois un défi majeur, marqué par un flou sémantique persistant dû à la multiplicité des approches théoriques et professionnelles (Kettani, 2021, p. 3 ; Lafrem & Benkaraache, 2021). En effet, le manque d'unification des cadres théoriques entre les approches processuelles, instrumentales et stratégiques fragilise la compréhension globale des enjeux liés à la sécurité des flux informationnels (Salvetat, 2011). Cette confusion sémantique est d'autant plus prégnante que les pratiques extrêmement agressives, parfois facilitées par des outils de surveillance à très large échelle, tendent à gommer les limites entre une intelligence économique orientée vers la résilience et des stratégies d'espionnage plus offensives. Cette mutation structurelle impose désormais d'intégrer l'usage de l'intelligence artificielle comme un catalyseur des menaces hybrides, capable d'amplifier radicalement l'impact des tactiques de déstabilisation et de captation de données (Nowicka et al., 2024, p. 494). En somme, cette omniprésence technologique impose de repenser la sécurité non plus comme un rempart statique, mais comme une capacité dynamique à naviguer dans une « zone grise » où la distinction entre compétition loyale et hostilité larvée devient structurellement indécidable (SANMORÌ, 2026; Weissmann, 2025).

5. Intelligence économique : entre veille, influence et sécurité économique

La fonction d'intelligence économique se déploie le long d'un continuum qui va de la veille licite, sur sources ouvertes, jusqu'à la captation clandestine. La typologie blanc, gris, noir en donne une représentation graduée, reprise par la Figure 3 et utilisée dans la suite comme repère de qualification (Baaziz, 2015, p. 126).

Figure 3. Continuum de l'intelligence économique à l'espionnage économique selon la typologie blanc, gris, noir.



Source : élaboration de l'auteur à partir de Baaziz (2015).

L'intelligence économique ne se réduit ni à la simple collecte d'informations ni à une fonction périphérique de l'organisation (Fontanel, 2004). Elle correspond à un mode de gouvernance fondé sur la maîtrise de l'information stratégique utile à la décision, à l'anticipation et à la défense des intérêts d'un acteur économique ou institutionnel(Dubeuf & Linck, 2012, p. 7). Dans cette perspective, elle articule trois dimensions complémentaires : la veille, l'influence et la sécurité économique (Laaroussi, 2015).

La veille constitue le socle opérationnel de cette démarche. Elle consiste à rechercher, sélectionner, analyser et diffuser des informations pertinentes sur l'environnement concurrentiel, technologique, réglementaire, géopolitique ou sociétal, afin de réduire l'incertitude et d'éclairer les choix stratégiques(Fasquelle, 2018, p. 127). L'objectif n'est pas l'accumulation de données, mais la production d'une connaissance exploitable, orientée vers l'anticipation des risques, la détection d'opportunités et l'adaptation rapide aux mutations de l'environnement (Fasquelle, 2018, p. 70).

Toutefois, l'intelligence économique ne saurait être confondue avec la veille seule. Dans l'acception la plus largement admise, elle inclut également une capacité d'action sur l'environnement, c'est-à-dire une logique d'influence (Shen, 2016, p. 28). Celle-ci renvoie à l'aptitude d'un acteur à orienter des perceptions, à peser sur des normes, à défendre ses intérêts dans les espaces décisionnels et à structurer un rapport de force favorable par l'usage maîtrisé de l'information (Caspar et al., 2009, p. 127). L'influence prolonge ainsi la connaissance par l'action et inscrit l'intelligence économique dans une dynamique de compétitivité et de puissance.

À cette double fonction d'observation et d'action s'ajoute une exigence de protection. La sécurité économique désigne l'ensemble des dispositifs destinés à préserver les actifs matériels et immatériels sensibles (Fontanel, 2016, p. 65), notamment les données stratégiques, le savoir-faire, la réputation, les réseaux de coopération et les capacités d'innovation (Fontanel, 2016, p. 7). Dans un contexte marqué par la vulnérabilité numérique, l'intensification des rivalités internationales et

la circulation accélérée de l'information, cette dimension défensive devient indissociable de toute politique d'intelligence économique (Damiano, 2019).

L'intérêt analytique de l'intelligence économique réside précisément dans l'articulation de ces trois fonctions. Veiller sans protéger expose l'organisation à la captation de ses ressources stratégiques ; protéger sans influencer limite sa capacité à agir sur son environnement (Laaroussi, 2015) ; influencer sans connaissance fiable affaiblit la qualité de la décision (Delbecque, 2020). L'intelligence économique apparaît ainsi comme un système intégré où l'information est à la fois ressource, levier d'action et objet de sécurisation.

En ce sens, l'intelligence économique s'inscrit pleinement dans les transformations de la compétition géo-économique contemporaine. Elle ne vise plus seulement à soutenir la performance des entreprises, mais aussi à renforcer leur résilience face aux rapports de puissance, aux asymétries informationnelles et aux formes diffuses de conflictualité économique(Bauer et al., 2020, p. 65). Elle devient dès lors un instrument central de lecture et de gestion des tensions entre coopération, concurrence et confrontation dans l'espace économique mondialisé.

6. De la protection à la prédation : l'espionnage économique comme versant clandestin de l'hybridité

L'espionnage économique désigne l'ensemble des pratiques offensives visant à obtenir, en dehors des voies licites, des informations sensibles détenues par une entreprise, une institution ou un État afin d'en tirer un avantage stratégique, commercial ou technologique (Zwolinska, 2015, p. 275). À la différence de l'intelligence économique, qui repose sur l'exploitation légale de l'information utile, l'espionnage économique se caractérise par l'illégitimité de ses procédés, qu'il s'agisse d'intrusion, de corruption, de détournement de données, de surveillance clandestine ou de captation de secrets d'affaires. La distinction entre les deux ne tient donc pas à la valeur de l'information recherchée, mais aux moyens mobilisés pour y accéder et à la finalité prédatrice qui oriente l'action (Zwolinska, 2015, p. 178).

Ce basculement de la protection vers la prédation s'inscrit dans un environnement concurrentiel profondément transformé par la numérisation, la mondialisation des chaînes de valeur et l'intensification des rivalités de puissance (Boulanger, n.d., p. 22). Dans ce contexte, l'information stratégique n'est plus seulement un facteur d'aide à la décision ; elle devient un objet de convoitise, susceptible d'être approprié, manipulé ou exploité pour affaiblir un concurrent, pénétrer un marché ou accélérer une acquisition technologique (Gabarre et al., 2021, p. 87). L'espionnage économique prend alors des formes multiples, allant du recrutement ciblé de personnels clés à la cyber-intrusion, en passant par l'interception de communications, la compromission de partenaires ou l'usage de structures intermédiaires destinées à masquer le commanditaire réel (Fontanel, 2016, p. 37).

L'un des apports majeurs de la notion d'hybridité est précisément de montrer que l'espionnage économique ne relève pas uniquement de pratiques clandestines isolées, mais d'un continuum plus large où interagissent des moyens légaux, ambigus et illégaux (Navarrete, 2016, p. 30). Des opérations d'influence, des pressions normatives, des asymétries technologiques ou des dépendances informationnelles peuvent préparer, couvrir ou prolonger des logiques de captation plus agressives. Dans cette perspective, l'espionnage économique apparaît comme le versant clandestin d'une conflictualité économique diffuse, où la frontière entre concurrence, renseignement et hostilité stratégique devient de plus en plus poreuse.

Une telle évolution impose de repenser la sécurité économique au-delà de la seule protection technique des données. Les vulnérabilités d'une organisation résident aussi dans ses ressources humaines, ses partenariats, son exposition numérique, sa gouvernance de l'information et sa capacité à identifier les signaux faibles d'une prédation en cours (Fontanel, 2016, p. 43). Étudier l'espionnage économique sous l'angle de l'hybridité permet ainsi de comprendre qu'il ne constitue pas une anomalie extérieure à l'intelligence économique, mais une possibilité de dérive inscrite dans le champ même de la compétition géo-économique lorsque la recherche d'avantage stratégique franchit le seuil de la légalité et de l'éthique.

7. La compétition géo-économique comme cadre stratégique de l'hybridité

Le concept de géoéconomie trouve son origine dans les travaux fondateurs d'Edward Luttwak, qui introduit le terme en 1990 pour désigner, à la fin de la Guerre froide, le glissement des rapports de puissance du terrain militaire vers le terrain économique : la géoéconomie y est définie comme « la logique du conflit avec la grammaire du commerce » (Luttwak, 1990, p. 19). En France, Pascal Lorot prolonge et systématise cette approche en définissant la géoéconomie comme « l'analyse des stratégies d'ordre économique, notamment commerciales, décidées par les États dans le cadre de politiques visant à protéger leur économie nationale » et à conquérir la suprématie technologique et commerciale (Lorot, 2009, p. 9).

La géoéconomie se distingue de la géopolitique traditionnelle sur trois plans. D'abord, la géopolitique pense la puissance à partir du contrôle de territoires physiques, tandis que la géoéconomie opère dans un espace « virtuel » ou fluidifié, affranchi des frontières, structuré par les flux, les chaînes de valeur et les marchés (Lorot, 2009, p. 11). Ensuite, sa finalité n'est plus la conquête territoriale, mais l'acquisition de la suprématie technologique et commerciale (Luttwak, 1990, p. 21). Enfin, ses acteurs privilégiés sont les États et les grandes entreprises à stratégie mondiale, davantage que les groupes humains territorialisés de la géopolitique classique (Csurgai, 2017). C'est dans cet espace déterritorialisé, où l'information et la technologie deviennent des ressources stratégiques de premier ordre, que l'hybridité trouve son terrain d'application privilégié.

La compétition géo-économique désigne une forme de rivalité dans laquelle les États, mais aussi les grandes entreprises et les blocs régionaux, mobilisent les ressources économiques, technologiques, financières et normatives pour accroître leur puissance ou défendre leurs intérêts stratégiques (Gabarre et al., 2021, p. 73). Dans cet espace, l'économie n'est plus un simple domaine d'échange ou de production de richesse ; elle devient un terrain d'affrontement structuré par des rapports de force, des dépendances asymétriques et des stratégies d'influence (Gabarre et al., 2021, p. 85). La géoéconomie apparaît ainsi comme une nouvelle grammaire de la puissance, dans laquelle l'accès aux marchés, la maîtrise des technologies, le contrôle des chaînes de valeur et la capacité à imposer des normes jouent un rôle central.

Dans ce cadre, l'hybridité prend tout son sens, car la confrontation géo-économique ne repose pas sur un seul instrument, mais sur la combinaison de moyens multiples et complémentaires (Romansky et al., 2024, p. 6). Sanctions, restrictions d'exportation, guerre des normes, politiques industrielles offensives, contrôle des infrastructures critiques, domination technologique ou captation de données s'imbriquent désormais dans des stratégies globales de puissance (Fontanel, 2020, p. 8). La conflictualité contemporaine se déploie donc dans une zone intermédiaire entre paix et affrontement ouvert, où l'économie sert à la fois de levier de pression, d'espace de concurrence et d'instrument de coercition.

L'information occupe une place décisive dans cette transformation. Dans un environnement marqué par l'interdépendance, la maîtrise des flux informationnels permet non seulement d'anticiper les mouvements adverses, mais aussi de façonner les conditions mêmes de la concurrence (Monino, 2013). L'intelligence économique s'inscrit alors dans une logique élargie de puissance, car elle contribue à l'identification des vulnérabilités, à la protection des intérêts stratégiques et à l'orientation des décisions dans un contexte où l'avantage compétitif dépend de plus en plus de la connaissance, de la donnée et de la capacité d'influence (Germon, 2013, p. 75).

C'est précisément cette centralité de l'information qui explique la porosité croissante entre intelligence économique, sécurité économique et espionnage économique. Lorsque la compétition géo-économique s'intensifie, la recherche d'avantage informationnel tend à dépasser le cadre de la veille légitime pour s'inscrire dans des pratiques plus offensives, ambiguës ou clandestines. L'hybridité ne doit donc pas être comprise comme une anomalie marginale, mais comme une caractéristique structurelle d'un ordre international dans lequel les rivalités de puissance se déploient de manière diffuse, continue et multidimensionnelle.

8. Instruments juridiques et technologiques au service de l'hybridité économique

L'hybridité économique repose désormais sur une convergence d'instruments juridiques et technologiques, démultipliant les capacités d'accès à l'information stratégique, d'orientation des rapports de force et de consolidation des positions dominantes. Dans cette dynamique, le droit s'affirme non plus comme un simple mécanisme de régulation neutre, mais comme un levier de puissance mobilisable au service de la compétition internationale (Serrurier & Moisan, 2017, p. 8). Certaines législations à portée extraterritoriale, notamment américaines, illustrent cette mutation en autorisant l'accès à des données détenues hors du territoire national par des entreprises soumises à leur juridiction (Bigo et al., 2019, p. 95).

Au premier rang de ces instruments, le FISA et le CLOUD Act sont au cœur des débats sur la souveraineté numérique et la sécurité économique. Si la section 702 de la FISA autorise la collecte de données sur des non-Américains situés à l'étranger à des fins de renseignement (Velliet, 2023, p. 26), le CLOUD Act permet aux autorités américaines d'exiger la communication de données stockées par des prestataires relevant du droit américain, quel que soit leur lieu physique d'hébergement (Bigo et al., 2019, p. 162). Cette synergie entre surveillance et extraterritorialité génère un risque structurel pour les organisations étrangères confiant leurs données sensibles à des infrastructures ou des prestataires assujettis à ces obligations légales.

La portée de ces dispositifs est décuplée par la centralité des infrastructures numériques contemporaines. Cloud, plateformes de communication, outils collaboratifs ou systèmes de stockage ne sont plus seulement des supports techniques : ils constituent des espaces stratégiques où se concentrent des données critiques pour l'innovation, les partenariats, les marchés et la prise de décision (Gil, 2022, p. 14). Dès lors, la dépendance envers des fournisseurs dominants engendre une vulnérabilité systémique : l'asymétrie durable dans le contrôle des données ne découle pas tant d'une collecte systématiquement avérée que de la simple possibilité, juridique et technique, d'y accéder.

Cette réalité souligne l'étroite imbrication entre outils technologiques, droit extraterritorial et hybridité économique. Si les instruments juridiques définissent le cadre d'autorisation ou de contrainte, les infrastructures technologiques permettent l'exploitation concrète de gisements informationnels devenus décisifs. L'hybridité naît ainsi de cette rencontre entre l'égalité formelle,

capacité technique et finalité stratégique, brouillant les frontières entre veille, sécurité économique, surveillance et prédation informationnelle.

9. Du legal à illegal : le continuum opérationnel entre intelligence économique et espionnage économique

L'une des difficultés majeures de l'analyse en intelligence économique réside dans la détermination de la frontière qui la sépare de l'espionnage économique. Si, en théorie, la distinction semble claire (l'intelligence économique relevant d'une recherche d'information dans un cadre légal, tandis que l'espionnage économique impliquerait une acquisition illicite de données protégées), cette séparation s'avère, en pratique, bien moins nette. De nombreuses activités évoluent en effet dans des zones intermédiaires où la licéité formelle, la légitimité éthique et l'intention stratégique ne coïncident pas systématiquement.

Cette zone grise est souvent illustrée par la typologie des sources d'information : l'information blanche, accessible ouvertement ; l'information grise, obtenue par des voies détournées mais licites ; et l'information noire, protégée et acquise illégalement (Baaziz, 2015, p. 126). Cette gradation démontre que le passage du légal à l'illégal ne s'opère pas nécessairement par une rupture brutale, mais plutôt par des glissements progressifs dans les méthodes de collecte, l'usage des réseaux, l'exploitation des vulnérabilités humaines ou l'intensification de la pression informationnelle (Carayol et al., 2020, p. 206). Le continuum opérationnel réside précisément dans cette progression, où des pratiques initialement admissibles peuvent servir de point d'entrée à des démarches plus intrusives.

Le concept de continuum permet de dépasser l'opposition binaire entre veille légitime et espionnage clandestin. Dans la réalité de la compétition économique, le renseignement s'appuie parfois sur des procédés d'observation agressifs, l'activation de réseaux informels, l'exploitation d'indiscrétions ou la collecte de données sensibles sans que l'illégalité soit immédiatement caractérisée (Goria, 2023, p. 88). Cette porosité suggère que l'intelligence économique peut, dans certaines configurations, constituer une passerelle vers des pratiques de prédation, notamment lorsque la pression concurrentielle, l'urgence stratégique ou la recherche d'un avantage décisif affaiblissent les garde-fous déontologiques.

Dans cette perspective, la question essentielle ne réside plus seulement dans la licéité stricte d'une pratique, mais dans l'identification du seuil à partir duquel elle devient un instrument offensif de captation informationnelle (Tenenbaum & Hartpence, 2015, p. 23). Le passage du légal à l'illégal doit ainsi être appréhendé comme un processus de déformation progressive des finalités et des moyens, où la quête d'information se mue en logique d'appropriation. Étudier ce continuum permet de mieux saisir la centralité de l'hybridité : la conflictualité géo-économique contemporaine ne se structure pas autour de catégories étanches, mais au sein d'une gradation mouvante entre surveillance, influence, renseignement et espionnage.

10. Hybridité, vulnérabilité et résilience des acteurs économiques

L'hybridité transforme profondément l'environnement de sécurité des acteurs économiques (Tikanmäki & Ruoslahti, 2022). Entreprises, administrations et opérateurs stratégiques ne font plus face à des menaces isolées, mais à des configurations de risque composites mêlant pression informationnelle, dépendance technologique, exposition juridique, vulnérabilité numérique et atteinte à la réputation (Freyssinet, 2025). Dans ce contexte, la sécurité économique doit être pensée

comme une capacité à contrer des attaques diffuses, souvent graduelles ; si elles n'empruntent pas nécessairement la forme d'une agression ouverte, elles peuvent fragiliser durablement l'autonomie décisionnelle d'une organisation.

Cette vulnérabilité tient, en premier lieu, à la centralité croissante de l'information stratégique dans la création de valeur (Goria, 2023, p. 85). Qu'il s'agisse de recherche, d'innovation, de contrats, de partenaires ou d'orientations de marché, ces données constituent désormais un patrimoine décisif dont la compromission affecte directement la compétitivité. L'intelligence économique rappelle, à cet égard, que la performance ne dépend pas seulement de la capacité à acquérir de l'information utile, mais aussi de l'aptitude à identifier, classer et protéger ses actifs les plus sensibles (Monino, 2013).

À cette dimension s'ajoute une vulnérabilité structurelle liée aux dépendances numériques. Le recours massif aux services cloud, logiciels critiques, plateformes collaboratives et chaînes d'approvisionnement internationales introduit des asymétries qui dépassent la simple efficacité technique (OECD, 2023). Ces dépendances engendrent des risques variés : surveillance, rupture de service, modification contractuelle unilatérale, perte de maîtrise opérationnelle et, plus largement, réduction de la souveraineté juridique et technologique des organisations.

Outre les fragilités techniques, les facteurs humains et organisationnels jouent un rôle prépondérant. L'ouverture des réseaux, la circulation élargie des données, la mobilité du personnel, l'externalisation de fonctions critiques ou encore l'effacement des frontières entre espace professionnel et privé multiplient les risques de fuite, de manipulation ou d'exploitation des informations (Desroches & Lefranc, 2020, p. 5). L'hybridité démontre ainsi que la vulnérabilité d'un acteur économique procède moins d'une faille isolée que d'un enchevêtrement de faiblesses internes et de pressions externes susceptibles d'être activées simultanément.

Dans ces conditions, la résilience ne se limite pas à une posture défensive ou à un empilement de dispositifs techniques ; elle renvoie à une capacité globale d'anticipation, d'absorption, d'adaptation et de continuité face à des perturbations multiples (Adjetey-Bahun, 2016, p. 34). Cela suppose une gouvernance intégrée de la sécurité économique, articulant cartographie des dépendances critiques, protection du patrimoine informationnel, culture du risque, formation des personnels et sécurisation des partenariats (OECD, 2021). Les approches récentes de résilience numérique insistent d'ailleurs sur la nécessité de mesurer et réduire ces dépendances pour préserver la continuité d'activité, la compétitivité et la sécurité économique (Griffe, 2022).

Ainsi comprise, la résilience devient le complément indispensable d'une lecture hybride de la compétition géo-économique. À mesure que les instruments de puissance s'insinuent dans les infrastructures, les normes et les flux informationnels, les acteurs économiques doivent renforcer leur capacité à conserver la maîtrise de leurs ressources essentielles (Fontanel, 2022, p. 164). L'enjeu n'est pas d'éliminer toute exposition au risque, ce qui serait illusoire, mais de construire une autonomie relative fondée sur la vigilance, la réversibilité, la protection des actifs stratégiques et l'aptitude à préserver une liberté de décision dans un environnement durablement conflictuel.

11. Conclusion : penser la gouvernance de l'hybridité dans la compétition géo-économique

L'examen de l'hybridité révèle que la frontière entre intelligence économique et espionnage économique est devenue poreuse, rendant obsolète leur perception comme des domaines étanches et immuables. Bien que l'intelligence économique repose théoriquement sur l'usage licite de l'information stratégique et l'espionnage sur des procédés clandestins ou illégaux, la dynamique

actuelle de la compétition géo-économique brouille ces clivages par l'émergence de zones grises et de dispositifs de captation indirects. Le concept d'hybridité s'avère donc indispensable pour saisir la continuité opérationnelle, ainsi que les tensions normatives, qui caractérisent la mutation de la veille stratégique vers des pratiques de prédation.

Cette perspective oblige à resituer l'intelligence économique au sein d'un cadre conflictuel qui excède la simple efficacité des organisations. Elle se trouve désormais à la convergence des enjeux de sécurité, de souveraineté informationnelle, de diplomatie et de guerre économique, dans un contexte où la donnée stratégique s'affirme comme un levier fondamental de puissance. Par conséquent, les activités d'influence, de surveillance et de protection doivent être examinées à la lumière des rivalités de puissance, des vulnérabilités technologiques et des nouvelles formes de confrontation qui définissent l'économie mondiale actuelle.

Il ressort de cette analyse que la transition entre les pratiques légales et illégales n'est généralement pas abrupte, mais résulte souvent d'une évolution graduelle des objectifs et des méthodes d'action. Lorsque la quête d'information est guidée par une volonté démesurée de gain compétitif ou de sécurité, elle risque de dépasser les limites de la légitimité juridique et morale. L'espionnage ne doit donc pas être perçu uniquement comme l'antithèse de l'intelligence économique, mais comme une dérive possible lorsque les structures de gouvernance et de responsabilité sont mises à mal par la pression exercée par la compétition internationale.

Ce constat souligne la nécessité de prioriser la sécurité économique et la résilience organisationnelle. Face à la rapidité des flux de données, à la fragilité des infrastructures numériques et à la montée en puissance de stratégies prédatrices sophistiquées, les acteurs économiques sont contraints d'accroître leurs capacités de défense et d'adaptation. L'objectif n'est pas simplement la protection d'actifs isolés, mais la préservation de la continuité décisionnelle et de l'autonomie stratégique, dans un environnement où l'information est simultanément une ressource, un vecteur d'attaque et un instrument de puissance.

Aborder la gouvernance de l'hybridité exige de concevoir des mécanismes intégrés alliant efficacité stratégique, respect des cadres juridiques, éthique et défense des intérêts vitaux. Une telle démarche nécessite d'abandonner le cloisonnement des pratiques, en articulant l'intelligence économique avec les problématiques de cybersécurité, de souveraineté numérique et de maîtrise des dépendances stratégiques. À terme, la valeur de l'intelligence économique ne dépendra pas seulement de l'optimisation de la collecte d'informations, mais de l'aptitude à réguler les conditions politiques, techniques et normatives de son utilisation au sein d'un écosystème géo-économique durablement marqué par l'hybridité.

Au terme de cette analyse, trois apports conceptuels peuvent être explicités. Premièrement, l'article enrichit la littérature sur l'intelligence économique en la réinsérant dans une lecture conflictuelle de la puissance, au-delà de la seule performance organisationnelle (Moinet & Bulinge, 2013; Delbecque, 2020). Deuxièmement, il propose de penser l'espionnage économique non comme l'antithèse de l'intelligence économique, mais comme une dérive inscrite dans un même continuum gradué, dont la typologie blanc, gris, noir constitue le révélateur (Baaziz, 2015, p. 126; Zwolinska, 2015, p. 178). Troisièmement, il opérationnalise la notion d'hybridité économique au moyen d'une grille à quatre dimensions, informationnelle, juridique, technologique et stratégique, qui articule la littérature sur les menaces hybrides à celle de la géoéconomie (Filipec, 2021; Csurgai, 2017). C'est de cette grille analytique que découlent directement les recommandations suivantes.

Les recommandations qui suivent procèdent directement de la grille et de l'étude de cas comparative. Chaque dimension positionnée au niveau gris ou noir appelle une réponse ciblée. Le Tableau 3 relie les dimensions, les constats issus des deux cas et les leviers d'action, par catégorie d'acteur. Cette traçabilité distingue les présentes recommandations d'une simple liste de bonnes pratiques.

Tableau 3. Recommandations dérivées de la grille et de l'étude de cas, par dimension et par acteur.

Dimension à risque	Constat issu de l'étude de cas	Levier d'action	Acteur principal
Juridique (niveau noir, cas A)	Exposition à l'extraterritorialité du droit étranger	Clauses de localisation et de réversibilité ; soutien aux solutions souveraines	Décideurs publics
Technologique (niveau noir, cas B ; gris, cas A)	Dépendance critique au cloud concentré et exploitation de vulnérabilités	Cartographie des dépendances ; diversification ; sécurité par conception	Entreprises et décideurs publics
Informationnelle (du blanc au noir)	Glissement de la veille vers la captation	Garde-fous déontologiques ; classification des actifs ; typologie blanc, gris, noir	Responsables de l'intelligence économique
Stratégique (du gris au noir)	Dilution de l'imputabilité ; finalité prédatrice	Gouvernance intégrée ; anticipation des signaux faibles ; résilience organisée	Décideurs publics et responsables IE

Source : élaboration de l'auteur à partir de l'analyse comparative du Tableau 2.

a. Recommandations à destination des entreprises

L'étude de cas place les entreprises face à deux risques principaux, technologique et informationnel. Sur le plan technologique, elles gagnent à cartographier leur exposition aux dépendances critiques et à négocier des clauses de réversibilité avec leurs prestataires, afin de réduire l'exposition observée dans le cas A (Gil, 2022, p. 14). Sur le plan informationnel, la classification des actifs immatériels sépare ce qui relève de la veille ouverte de ce qui exige une protection renforcée (Goria, 2023, p. 85). Une culture du risque, attentive aux signaux faibles de prédation, complète ce dispositif (Desroches & Lefranc, 2020, p. 5).

b. Recommandations à destination des décideurs publics

Le cas A désigne le risque juridique comme le plus aigu pour la puissance publique. La réponse passe par des dispositifs réduisant l'exposition à l'extraterritorialité du droit étranger et par le soutien à des solutions de souveraineté numérique (Bigo et al., 2019, p. 162). Sur le plan stratégique, une gouvernance intégrée de la sécurité économique articule cartographie des dépendances, protection du patrimoine informationnel et sécurisation des chaînes d'approvisionnement (OECD, 2021 ; Fontanel, 2022, p. 164). L'encadrement de l'intelligence artificielle comme catalyseur de menaces hybrides relève de la même logique d'anticipation (Nowicka et al., 2024, p. 494).

c. Recommandations à destination des responsables de l'intelligence économique

La grille assigne aux responsables de l'intelligence économique un rôle de qualification. Sur le plan déontologique, ils peuvent formaliser des garde-fous prévenant le glissement de la veille vers la captation, en utilisant la typologie blanc, gris, noir comme outil de qualification opérationnel (Baaziz, 2015, p. 126). Sur le plan stratégique, ils positionnent la fonction comme pivot d'une résilience organisée, capable d'anticiper, d'absorber et de s'adapter aux perturbations (Adjetey-Bahun, 2016, p. 34). La formation des personnels et la sécurisation des partenariats réduisent les vulnérabilités humaines activables (Langen et al., 2024, p. 344).

12. Références

- Adjetey-Bahun, K. (2016). *End-to-end resilience for the (re)designing of a transportation system*. http://www.theses.fr/2016TROY0012/document
- Baaziz, A. (2015). Synergie du triptyque : Knowledge Management, Intelligence Economique et Business Intelligence. Contribution à la réduction des risques liés aux décisions stratégiques dans les nouveaux environnements concurrentiels incertains : Cas des Entreprises Publiques Algériennes. In *theses.fr (ABES)*. http://www.theses.fr/2015AIXM5900/document
- Bauer, A., Faron, O., Richier, J., Bar-Hen, A., Béra, M., Cappelletti, L., Collomb, A., Durance, P., Fleury-Perkins, C., Fontanet, A., Gnesotto, N., Réau, B., & Trainar, P. (2020). Chaire Nouveaux risques : rapport 2020. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://cnam.hal.science/hal-03249874
- Bigo, D., Isin, E. F., & Ruppert, E. (2019). Data Politics. Worlds, Subjects, Rights. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://sciencespo.hal.science/hal-03385170
- Boulanger, P. (n.d.). *Planète médias*.
- Carayol, V., Lépine, V., & Morillon, L. (2020). Le côté obscur de la communication des organisations. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/hal-02525979
- Caspar, R., Besnard, F., Dhérissard, G., Salaun, G., & Wallet, F. (2009). Revenir au territoire, un enjeu pour le développement. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/hal-01198037
- Chtouki, Z., & Deriouch, K. (2020). Intelligence économique au regard de l'éthique : Synthèse de débats théorique. *PRSM*, *9*(1), 193–207. https://doi.org/10.34874/imist.prsm/doreg-v9i1.21193
- Commission européenne (2019). *The scale and impact of industrial espionage and theft of trade secrets through cyber*. Bruxelles : Direction générale du marché intérieur, de l'industrie, de l'entrepreneuriat et des PME. https://ec.europa.eu/docsroom/documents/34841
- Csurgai, G. (2017). The Increasing Importance of Geoeconomics in Power Rivalries in the Twenty-First Century. *Geopolitics*, *23*(1), 38–46. https://doi.org/10.1080/14650045.2017.1359547
- Damiano, J.-P. (2019). *Les enjeux de la recherche et l'intelligence économique et stratégique*. https://doi.org/10.51257/a-v1-ag1611

- Delbecque, É. (2020). L'anticipation et la sûreté des organisations. *Prospective et stratégie*, *1*, 63–72. https://doi.org/10.3917/pstrat.010.0063
- Desroches, V., & Lefranc, S. (2020). La menace cyber au coeur de la transition numérique. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/hal-03463073
- Dubeuf, J.-P., & Linck, T. (2012). Economic Intelligence for pastoral activities in the Mediterranean areas: strategic survey, territorial prospective and governance. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.inrae.fr/hal-02804911
- Fasquelle, J. (2018). Environmental scanning as a support to technological innovation. In *theses.fr (ABES)*. http://www.theses.fr/2018GREAG005/document
- Feige, J., Fane, O., & Bidi, G. (2024). Espionnage industriel et intelligence économique : cadre d'analyse d'une délimitation. *SPIRE - Sciences Po Institutional REpository*, *1*, 134–151. https://doi.org/10.3917/mss.036.0134
- Filipec, O. (2021). Preventing Hybrid Threats: From Identification to an Effective Response. *European Studies. The Review of European Law, Economics and Politics*, *8*(1), 17–38. https://doi.org/10.2478/eustu-2022-0063
- Fontanel, J. (2004). L'intelligence économique et son exercice. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.univ-grenoble-alpes.fr/hal-02196523
- Fontanel, J. (2016). La sécurité économique et sociétale. In *Paix et sécurité européenne et internationale*. https://doi.org/10.61953/psei.978
- Fontanel, J. (2020). Les conflits économiques. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.univ-grenoble-alpes.fr/hal-03112668
- Fontanel, J. (2022). Globalization and recurrent crises. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.univ-grenoble-alpes.fr/hal-03703460
- Freyssinet, É. (2025). Évolution des menaces de cybersécurité en 2025. *Enjeux Numériques.*, *4*, 9–13. https://doi.org/10.3917/ennu.032.0009
- Gabarre, É., Boudinot, F., Wiel, N., Pierron, M., Compo, N., & Paraire, P. (2021). *Géopolitique des relations internationales*.
- Georgelin, E., & Holeindre, J.-V. (2021). Des ruses de guerre numériques ? Le hacking comme ressource stratégique dans les conflits contemporains. *Industrias Culturais (Universidade de Coimbra)*, *103*, 89–104. https://doi.org/10.4000/quaderni.2020
- Germon, R. (2013). Protect the intangible capital of small and medium size enterprises : to a tool for decision making. In *theses.fr (ABES)*. http://www.theses.fr/2013TROY0019/document
- Gil, L. R. A. (2022). The governance of data as "commons" : a legal-strategic study for a public valorisation of informational data. In *theses.fr (ABES)*. http://www.theses.fr/2022ULILD018/document
- Goria, S. (2023). From information to product innovation : development of studies at the crossroads of strategic intelligence, knowledge management and forms of games used for serious purposes. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/tel-04090091

- Griffe, S. (2022). La résilience numérique, un sport d'équipe, et une affaire de bon sens. *Revue Défense Nationale*, *10*, 29–36. https://doi.org/10.3917/rdna.855.0029
- GROS, D., & VILBOUX, N. (2021). *La stratégie des États-Unis face aux menaces hybrides*.
- Hamel, T. (2025). Technologies numériques et sécurité : vers une recomposition du champ stratégique ? *Sécurité Globale*, *4*, 5–26. https://doi.org/10.54695/secug.254.0007
- IP Commission (2017). *Update to the IP Commission Report: The Theft of American Intellectual Property*. The National Bureau of Asian Research. https://www.nbr.org/wp-content/uploads/pdfs/publications/IP_Commission_Report_Update.pdf
- Kettani, Z. (2021). Apports de l'intelligence économique à la compétitivité des établissements hôteliers. In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/hal-03433561
- Kovalchuk, M. A. (2025). Гібридні загрози та економічний примус: сучасні виклики економічній безпеці у цифровому середовищі. *Вісник Академії Праці, Соціальних Відносин і Туризму. Серія: Економіка, Психологія Та Управління.*, *5*. https://doi.org/10.54929/3041-2390-2025-05-01-04
- Laaroussi, R. (2015). *La Communauté Intelligence Economique*. http://ui06.com/jcms/prd_576573/fr/la-communaute-de-ressources-en-intelligence-competitive-cric
- Lafrem, M., & Benkaraache, T. (2021). L'intelligence économique dans la littérature : Une contribution à la réflexion. *Zenodo (CERN European Organization for Nuclear Research)*, *4*(3). https://doi.org/10.5281/zenodo.5152422
- Langen, P. W. de, Constante, J. M., & Pruñonosa, S. F. (2024). Les (éco)systèmes d'innovation dans les ports:Une analyse comparative des ports de Rotterdam et de Valence. *CBS Research Portal (Copenhagen Business School)*. https://research.cbs.dk/en/publications/5405e43e-041b-41ef-be60-79e05b5d2b83
- Lorot, P. (2009). La géoéconomie, nouvelle grammaire des rivalités internationales. *L'Information géographique*, 73(3), 9–19. https://doi.org/10.3917/lig.733.0009
- Luttwak, E. N. (1990). From Geopolitics to Geo-Economics: Logic of Conflict, Grammar of Commerce. *The National Interest*, 20, 17–23. https://www.jstor.org/stable/42894676
- Mazur, I. (2025). HYBRID THREATS AND ECONOMIC RESILIENCE IN THE CONTEXT OF DIGITAL TRANSFORMATION. *Book of Abstracts*, 103–104. https://doi.org/10.36690/iceaf-2025-103-104
- Moinet, N., & Bulinge, F. (2013). Intelligence économique : vers une nouvelle dynamique de recherche. *Revue française des sciences de l'information et de la communication*, *3*. https://doi.org/10.4000/rfsic.598
- Monino, J. (2013). L'information au cœur de l'intelligence économique stratégique. *Marché et organisations*, *2*, 25–39. https://doi.org/10.3917/maorg.018.0025
- Navarrete, I. (2016). L'espionnage en temps de paix en droit international public. *Canadian Yearbook of international Law/Annuaire canadien de droit international*, *53*, 1–65. https://doi.org/10.1017/cyl.2016.16
- Nowicka, J., Ciekanowski, Z., Czternastek, M., Król, A., & Kacprzak, M. (2024). Navigating Hybrid Threats: Advanced Security Solutions for Modern Organizations. *EUROPEAN RESEARCH STUDIES JOURNAL*, 488–499. https://doi.org/10.35808/ersj/3414

- Ocqueteau, F. (2012). Existe-t-il un droit à une vie privée dans l'entreprise à l'heure de la guerre économique ? In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://hal.science/hal-00805561
- ODNI (2025). *Annual Statistical Transparency Report Regarding the Intelligence Community's Use of National Security Surveillance Authorities, Calendar Year 2024*. Office of the Director of National Intelligence. https://www.dni.gov/files/CLPT/documents/2025_ASTR_for_CY2024.pdf
- OECD. (2021). Gouvernance de la Résilience des Infrastructures Critiques. In *Panorama des administrations publiques*. Organization for Economic Cooperation and Development. https://doi.org/10.1787/2d9041c8-fr
- OECD. (2023). Résumé. In *OECD skills studies*. Organization for Economic Cooperation and Development. https://doi.org/10.1787/a7395c9d-fr
- Razinkina, I., Bulatenko, M., Chernov, S., & Prasolov, V. (2022). Ethical and legal balance of modern economic intelligence. *The Journal of World Intellectual Property*, *25*(2), 335–346. https://doi.org/10.1111/jwip.12225
- Romansky, S., Hoenig, A., Meessen, R., Kruijver, K., Sweijs, T., van Weerd, C., & Bekkers, F. (2024). *New Technologies, Changing Strategies: Five Trends in the Hybrid Threat Landscape*.
- Salvetat, D. (2011). Les approches théoriques et l'influence sur la sécurité des pratiques d'intelligence économique dans les entreprises européennes de hautes technologies. *Revue Française de Gestion Industrielle*, *30*(2), 53–66. https://doi.org/10.53102/2011.30.02.815
- SANMORÌ, M. (2026). L'uomo al centro della guerra ibrida. Dal cyberspazio alla guerra cognitiva nell'era dell'intelligenza artificiale. *Electronic Theses and Dissertations Repository (University of Pisa)*. http://etd.adm.unipi.it/theses/available/etd-12162025-154135/
- Schmid, J. C., & Georget, J.-L. (2021). Considérations sur la guerre hybride. *Allemagne d aujourd hui*, *1*, 141–148. https://doi.org/10.3917/all.235.0141
- Serrurier, E., & Moisan, C. (2017). "Is International Law at the Service of Powerful States?" In *HAL (Le Centre pour la Communication Scientifique Directe)*. Centre National de la Recherche Scientifique. https://uca.hal.science/hal-01679594
- Shen, L. (2016). *Textometric Multilingual Information Monitoring Methods Applied to Energy & Environment Corpora : "Restitution, Forecasting and Anticipation of Events by Cross Poly-resonance."* http://www.theses.fr/2016USPCA085/document
- Synergy Research Group (2025). *Cloud Market Share Trends: The Big Three Together Hold 63%*. https://www.srgresearch.com/articles/cloud-market-share-trends-big-three-together-hold-63-while-oracle-and-the-neoclouds-inch-higher
- Tenenbaum, E., & Hartpence, P. (2015). *Le piège de la guerre hybride*.
- Tikanmäki, I., & Ruoslahti, H. (2022). How are Hybrid Terms Discussed in the Recent Scholarly Literature? *European Conference on Cyber Warfare and Security*, *21*(1), 296–304. https://doi.org/10.34190/eccws.21.1.457
- U.S. Department of Justice (2024). *Report to Congress on the Implementation of the U.S.-U.K. CLOUD Act Agreement*. Washington : Department of Justice.
- Urtmelidze, T. (2025). The role of intellectual property in addressing state security challenges. *DergiPark (Istanbul University)*. https://doi.org/10.5281/zenodo.15023899

- Velliet, M. (2023). Souveraineté numérique : politiques européennes, dilemmes américains. In *HAL AMU*. https://hal.science/hal-03968950
- Vitanovski, S., & Taneski, N. (2025a). CHALLENGES FOR SECURITY AND INTELLIGENCE AGENCIES IN DEALING WITH HYBRID THREATS. In *Zenodo (CERN European Organization for Nuclear Research)*. European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.18959436
- Vitanovski, S., & Taneski, N. (2025b). CHALLENGES FOR SECURITY AND INTELLIGENCE AGENCIES IN DEALING WITH HYBRID THREATS. In *Zenodo (CERN European Organization for Nuclear Research)*. European Organization for Nuclear Research. https://doi.org/10.5281/zenodo.18959435
- Weissmann, M. (2025). Future threat landscapes: The impact on intelligence and security services. *Security and Defence Quarterly*. https://doi.org/10.35467/sdq/197248
- Weissmann, M., Nilsson, N., Palmertz, B., & Thunholm, P. (2021). *Hybrid Warfare Security and Asymmetric Conflict in International Relations*.
- Zwolinska, M. (2015). *Security and Fundamental Freedoms of Electronic Communications in French, European and International Law*. http://www.theses.fr/2015NICE0038/document