ChatGPT

État des lieux de l'intelligence économique en Belgique

L'**intelligence économique (IE)** désigne la collecte, l'analyse et la protection de l'information stratégique pour la compétitivité. En Belgique, le dispositif est peu centralisé : il mobilise principalement des organes dispersés au niveau fédéral et régional, mais pas de « pivôt » national unique. Au niveau fédéral, la **Sûreté de l'État (VSSE)** assure la contre-espionnage économique et la protection du *potentiel scientifique et économique* (WEP) contre les ingérences étrangères [1]. Elle alerte notamment sur la menace d'espionnage chinois ciblant la propriété intellectuelle des entreprises belges [1]. De son côté, le **SPF Économie (Économie-PME)** a mis en place des dispositifs de cybersécurité (point de contact « Meldpunt », application de la directive NIS) et prévoit de renforcer la sécurité numérique des PME en collaboration avec le Centre pour la Cybersécurité (CCB) [2]. Le SPF Affaires étrangères coordonne la diplomatie économique (attachés commerciaux, conseillers économiques) mais sans orientation spécifique IE. Enfin, la Belgique a transposé en 2018 la directive européenne sur le **secret des affaires** : la loi du 30 juillet 2018 offre un cadre légal de protection renforcée des savoir-faire sensibles [3].

Aux niveaux régionaux et communautaires, plusieurs initiatives existent. En Wallonie, le Plan Marshall 2.Vert (2013) a confié à l'Agence de Stimulation Économique (ASE) un dispositif *d'intelligence stratégique* pour les PME. Celui-ci combine sensibilisation, formation et accompagnement selon trois piliers – veille stratégique, protection de l'information et influence – destinés à renforcer la compétitivité des entreprises wallonnes [4]. À Bruxelles, l'agence hub.brussels (fusion de Bruxelles Économie & Emploi et Brussels Invest & Export) anime des services d'appui à l'exportation et la mise en réseau des entreprises, mais sans structure IE formalisée. En Flandre, les organismes VLAIO (Innovation), Flanders Investment & Trade, ainsi que les *speerpuntclusters* régionaux soutiennent l'innovation et l'export, avec un fort accent sur l'Industrie 4.0 et la cybersécurité, mais ils n'ont pas de mission explicite d'« IE » au sens stratégique. Les Communautés (francophone et flamande) et leurs agences (Wallonia-Brussels International, e.a.) encouragent la R&D et les technologies, notamment via l'export de services et le financement d'étudiants, ce qui complète indirectement l'effort d'intelligence économique.

Enfin, du côté privé, des **conseillers** (consultants IE), des *chambres de commerce* et des associations professionnelles (p.ex. VOKA, UCM) offrent formation et veille aux entreprises. Un réseau de **conseillers en diplomatie économique** bénévoles (min. Affaires étrangères) informe les ambassades sur l'environnement économique local [5]. Toutefois, la plupart des PME belges demeurent mal informées des risques d'espionnage industriel et de cyberattaques, et leur recours aux aides publiques d'IE est marginal.

Lacunes et faiblesses du dispositif belge

La fragmentation institutionnelle belge crée plusieurs points faibles. D'une part, l'absence d'une instance nationale unique d'IE (à la différence d'un SISSE français) rend la coordination difficile. Les informations stratégiques sont partagées tardivement entre services (VSSE, SPF Économie, etc.) et régions, ce qui peut laisser des « angles morts » de surveillance. Par exemple, les PME étrangères signalent rarement aux autorités belg es des cyberincidents ou tentatives d'espionnage : le **Meldpunt** du SPF Économie existe, mais son usage reste très marginal. D'autre part, les ressources allouées restent limitées. Les services publics de sécurité (VSSE, SGRS) font face à de multiples priorités

(terrorisme, cybersécurité…), ce qui limite l'attention portée aux menaces économiques. Le personnel dédié à l'IE dans l'administration est resté mince, et la sensibilisation des cadres (par exemple via la formation) est peu systématique. Au niveau légal, si la loi « secrets d'affaires » est en place (2018) [3], il n'existe pas d'équivalent d'une « loi renseignement économique » imposant des obligations de vigilance dans les appels d'offres publics (comme le propose un projet en France [6]). En outre, la Belgique n'a pas de dispositif formel de **screening des investissements étrangers** avant 2023 ; on note seulement que la VSSE participe désormais à un tel processus pour les secteurs critiques [7], mais ce mécanisme est récent.

Sur le plan opérationnel, les entreprises belges manquent souvent de culture IE. Elles investissent peu dans la veille stratégique ou la sécurité de leur information (plutôt réactive que proactive). Les petits pays voisins (France, Pays-Bas) sont perçus comme des marchés prioritaires, d'où une tendance à « oublier » le risque d'espionnage économique à l'étranger. Par exemple, un audit interne a révélé récemment que des **hackers chinois** ont siphonné environ 10 % des courriels externes de la Sûreté de l'État entre 2021 et 2023 [8]. Ce grave incident (dit « affaire Barracuda ») a exposé des failles dans la protection d'une institution clé, montrant la vulnérabilité aux cybermenaces transnationales. Les entreprises n'ont pas de remparts publics équivalents pour les alertes cybersécurité : bien que la Belgique ait lancé une Stratégie Cyber 2021–2025 (CCB) et aide ponctuellement les PME via des formations locales, la majorité des PME reste peu préparée (vol de données client, ransomware, etc.).

Exemples récents : bonnes pratiques et manquements

Bonne pratique (Wallonie – *Intelligence Stratégique*) : le programme lancé par l'ASE en Wallonie constitue un modèle de sensibilisation structurée. En phase pilote (2008) puis généralisée (2013), il a formé et accompagné des dizaines de PME dans l'analyse de leur environnement (veille concurrentielle), la sécurisation de l'information (confidentialité, plan de continuité) et la veille technologique [4]. Cette approche intégrant « veille, protection et influence » permet aux PME wallonnes de mieux anticiper les opportunités et menaces (par ex. repérer une OPA hostile sur un client ou un fournisseur). Ce dispositif régional est unique en Belgique et a produit des guides pratiques (études de cas, recommandations) partagés lors des « Assises de l'IS ».

Manquement notable (cybersécurité nationale) : l'incident des emails de la Sûreté de l'État volés par la Chine [8] illustre un manque de résilience. Pendant deux ans (2021–2023), des pirates liés aux services de renseignement chinois ont exploité une vulnérabilité d'un logiciel de sécurité tiers (Barracuda) pour intercepter massivement des communications de la VSSE – l'un des plus graves piratages jamais connus de ce service [8]. Cette fuite de courriels stratégiques (relations avec ministères, enquêtes) souligne qu'une dépendance envers des technologies importées et une réaction tardive peuvent compromettre la protection des informations sensibles. Dans le secteur privé, bien que moins médiatisée, on observe souvent des transferts de données vers des serveurs cloud hors de l'UE sans évaluation des risques, ce qui expose les savoir-faire belges (par exemple en biotechnologie, logistique) aux programmes de la NSA ou du FSB.

Comparaisons internationales

- **France** (dispositif étatique structuré) : l'État français a créé en 2016 le *Service de l'Information Stratégique et de la Sécurité Économiques (SISSE)*, intégré à la Direction générale des Entreprises. Le SISSE opère au niveau national (sous autorité d'un commissaire) et dispose d'un réseau de

délégués à l'information stratégique (DISSE) dans chaque région (sous l'autorité des préfets) [9] [10]. Ces DISSE coordonnent localement l'IE territoriale, conseillent les PME, effectuent la veille et détectent les menaces (OPA, cyber-attaques) sur les actifs stratégiques. Par exemple, ils renseignent la liste des « entreprises stratégiques » et gèrent le contrôle des investissements étrangers (FI). L'État français a également renforcé la protection juridique (loi « de blocage » de 1968, loi renseignement de 2017). En résumé, la France mise sur une **structure étatique forte et centralisée** d'IE, soutenue par des conseillers et des publications pédagogiques (guides de sécurité en 28 fiches [10]).

- **Allemagne** (modèle PME/clusters) : l'Allemagne ne dispose pas d'un service unique d'IE, mais s'appuie sur son tissu de *Mittelstand* (PME familiales) et un solide écosystème d'innovation. L'État fédéral et les Länder soutiennent massivement la R&D et la formation technique : par exemple, via le programme ZIM (centres d'innovation pour PME) et l'initiative *Mittelstand-Digital*. Le pays compte plus de 99 % de PME – souvent « champions cachés » à l'international – qui innovent énormément (forte part de brevets) [11]. Les politiques publiques allemandes favorisent la formation duale (atout pour les compétences) et le transfert de technologie (Fraunhofer, Helmholtz, clusters Industrie 4.0), ce qui renforce la compétitivité des entreprises et les rend naturellement résilientes. La promotion explicite des PME reste un pilier central en Allemagne : « des programmes de soutien à la recherche, à la numérisation des petites entreprises et à la formation… sont des piliers essentiels… pour garantir la position des PME et les développer [11]. »

Les différences clefs sont donc : en France l'**IE est pilotée par l'État** avec un réseau hiérarchisé (SISSE/DISSE), alors qu'en Belgique l'approche est fragmentée entre niveaux fédéral et régional sans organe unique. L'Allemagne, quant à elle, mise plutôt sur l'**excellence des PME** et sur la coopération entre industrie et recherche (Fraunhofer, pôles) plus que sur un dispositif politique spécifique.

Recommandations pour renforcer la résilience économique belge

1. **Créer une coordination nationale de l'IE**. S'inspirer du modèle français en établissant un service fédéral dédié (ou un guichet unique) chargé de centraliser le renseignement économique et la protection stratégique. Ce "centre" pourrait agréger les alertes de la VSSE, du CCB et des régionales, puis diffuser des conseils aux entreprises. On pourrait également instituer périodiquement une « conférence annuelle IE » réunissant État, Régions et acteurs privés pour partager veille et bonnes pratiques.

2. **Renforcer la sensibilisation des entreprises et des administrations**. Développer des outils pédagogiques (guides, formations obligatoires, fiches pratiques) sur la sécurité économique et la veille stratégique. Par exemple, diffuser aux PME un *kit de sécurité économique* (inspiré des "28 fiches" françaises [10]), et intégrer une sensibilisation à l'IE dans les cursus techniques (écoles d'ingénieurs, business schools) afin que les gestionnaires identifient mieux leurs actifs stratégiques.

3. **Améliorer la protection juridique et réglementaire**. Compléter la loi secrets d'affaires (2018) par des mesures préventives : exiger des garanties de non-divulgation dans les marchés publics sensibles, comme envisagé par le projet français de « plan national IE » [12]. Généraliser le screening des investissements étrangers initié en 2023 [7] et étendre sa portée aux PME innovantes (afin de décourager les rachats oppoprtunistes). Clarifier les responsabilités en

matière de cybersécurité (ex. exigences de certification, de notification des fuites) pour les PME et collectivités stratégiques.

4. **Développer l'appui aux PME**. Renforcer les agences régionales (ASE, VLAIO, hub.brussels) en dotant chacune d'experts en IE/informations stratégiques. Par exemple, créer des « délégués IE » dans chaque Région (comme les DISSE français) ou des cellules de veille dans les chambres de commerce pour accompagner les PME à l'export et dans le numérique. Encourager les clusters technologiques (sécurité, énergie, digital) à intégrer des modules de veille stratégique pour stimuler l'intelligence collective du territoire.

5. **Accroître la coopération internationale et européenne**. Intensifier les échanges d'information stratégiques avec les partenaires (France, Pays-Bas, UE). Participer activement aux réseaux européens de sécurité économique. Au sein de l'OTAN ou de l'UE, réclamer des appuis (ex. alertes précoces) pour protéger les savoir-faire belges critiques. Enfin, promouvoir à l'étranger le rôle de la Belgique (petit État) comme hub logistique et cyber, ce qui pourrait attirer des soutiens en retour en matière de veille.

Ces mesures contribueraient à consolider la **compétitivité nationale** en assurant la protection des actifs stratégiques et en renforçant la **résilience économique** belge. Dans un contexte de rivalités technologiques croissantes, disposer d'un dispositif cohérent d'intelligence économique (coordiné, préventif, et orienté PME) est vital pour sécuriser les emplois et l'innovation en Belgique.

<!-- ### Comparatif succinct Belg./France/All.
Aspect	Belgique	France	Allemagne
Coordination centrale	Modèle fragmenté (VSSE, SPF Éco, Régions)	SISSE (DGE) + réseau régional DISSE [9]	État fédéral/Länder, pas de SISSE		**Législation clef**	Loi « secrets d'affaires » 2018 [3]	Lois renseig. (2017), « blocage » 1968, IE 2022	Loi « GeschGehG » 2019 (directive UE)		**Soutien aux PME**	Initiatives d'animation (clusters, VLAIO, ASE)	DISSE conseillent localement, guides pratiques [10]	Subventions R&D (ZIM), formation duale		**Ex. de bonne pratique**	Dispositif wallon d'IE (Plan Marshall) [4]	SISSE centralisé, plans de sécurité économique	Innovation et clusters Industrie 4.0	-->

---

[1] Les milieux extrémistes surveillés de près par la Sûreté de l'État | Belgique | 7sur7.be
https://www.7sur7.be/belgique/les-milieux-extremistes-surveilles-de-pres-par-la-surete-de-l-etat~aac42a86/

[2] ccb.belgium.be
https://ccb.belgium.be/sites/default/files/2024-10/CCB_Strategie%202.0_FR_DP2.pdf

[3] Secrets d'affaires : protection par le secret d'invention, du savoir-faire ou d'informations | SPF Economie
https://economie.fgov.be/fr/themes/propriete-intellectuelle/droits-de-propriete/regimes-de-protection/secrets-daffaires-protection

[4] Le Parlement de Wallonie
https://www.parlement-wallonie.be/pwpages?p=interp-questions-voir&type=28&iddoc=46993

[5] Conseillers en diplomatie économique | SPF Affaires étrangères - Commerce extérieur et Coopération au Développement
http://diplomatie.belgium.be/fr/politique/diplomatie-economique/conseillers-en-diplomatie-economique

[6] [12] Programme national d'intelligence économique
https://www.senat.fr/leg/ppl20-489.html

7 Intelligence report 2023 | VSSE
https://www.vsse.be/fr/intelligence-report-2023

8 Des mails des renseignements belges “siphonnés” par des hackeurs chinois
https://www.courrierinternational.com/article/securite-des-mails-des-renseignements-belges-siphonnes-par-des-hackeurs-chinois_228178

9 10 Protéger les entreprises et l'économie française | Direction générale des Entreprises
https://www.entreprises.gouv.fr/la-dge/nos-missions/proteger-les-entreprises-et-leconomie-francaise

11 L'Allemagne est un pays de PME 🏭 champions cachés 🏆 de cœur ❤ et d'innovation du milieu, de la classe moyenne
https://xpert.digital/fr/pays-kmu-allemagne/