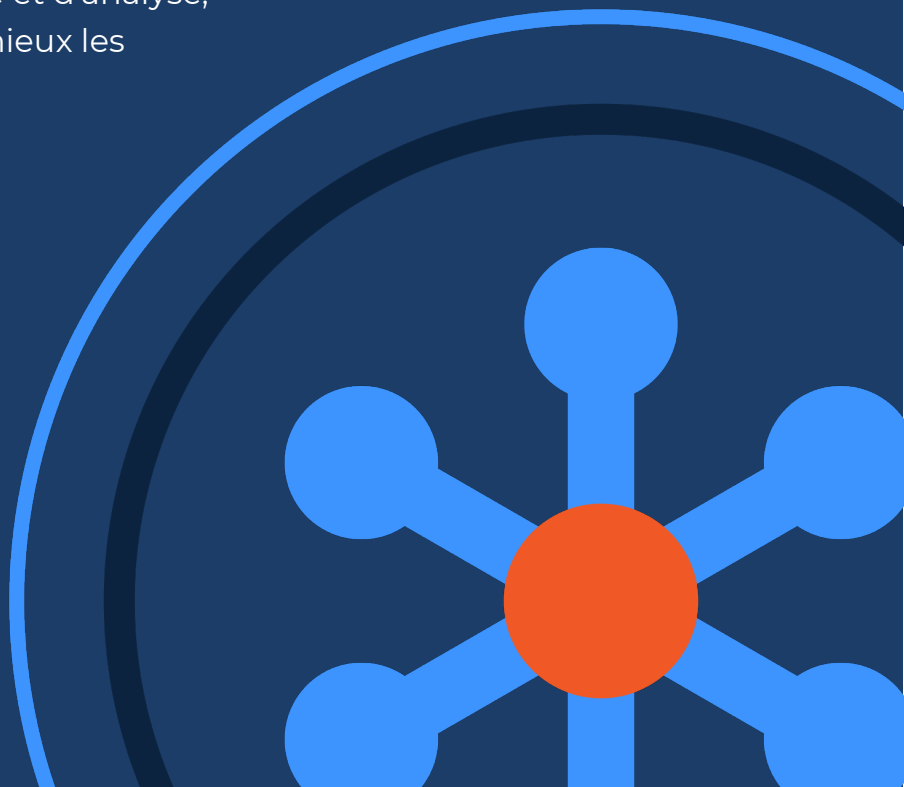




// VEILLE TRIMESTRIELLE

OBSERVATOIRE DES **MENACES** **HYBRIDES**

Face à l'explosion des ingérences qui menacent la sécurité économique des entreprises, l'Observatoire des menaces hybrides, plateforme indépendante de veille et d'analyse, permet de les comprendre pour mieux les prévenir et les gérer.





SÉCURITÉ ÉCONOMIQUE : LES ENTREPRISES EN PREMIÈRE LIGNE

Des PME aux grands groupes : les entreprises de plus en plus exposées, face à des alertes de sécurité économique plus nombreuses, plus étendues, plus diverses dans leurs origines et plus variées dans leurs modes opératoires.

SÉQUENCE RESSERRÉE

- Cession de LMB Aerospace à un groupe américain**
Fin 2025
- Rapport parlementaire : La Sécurité économique de la France**
Juillet 2026
- Assises de la sécurité économique**
24 sept.
- Doctrine de sécurité économique de la France**
24 sept.

En 2025, 750 alertes de sécurité économique ont été traitées par le SISSE, soit trois fois plus qu'il y a cinq ans, et la tendance se confirme en 2026. Dans la base industrielle et les technologies de défense, 80 % des dossiers traités concernent des PME ou des ETI, qui, selon Bercy, représentent souvent le maillon faible, faute de moyens de protection internes comparables à ceux des grands groupes.

Cette hausse s'inscrit dans une séquence institutionnelle resserrée. Un rapport parlementaire dressant un état des lieux du dispositif français de sécurité économique, publié en juillet, a précédé les assises, tenues le 24 septembre, jour où la doctrine de sécurité économique de la France a également été publiée.

Le secrétaire général de la défense et de la sécurité nationale y a présenté neuf familles de menaces hybrides déjà identifiées dans la Revue nationale stratégique 2025, dont la massification était anticipée.

750

alertes de sécurité économique traitées par le SISSE en 2025 = x3 en cinq ans

Neuf familles de menaces identifiées par le SGDSN

CAPITAL

Attaques capitalistiques et financières

CAPITAL

Chaînes de valeur et approvisionnements

PERSONNES

Espionnage et captation de technologies

PERSONNES

Débauchage et ingénierie sociale

INFO & DROIT

Manipulation de l'information

INFO & DROIT

Lawfare, contentieux, audits abusifs

SYSTÈMES

Cyberattaques et fuites de données

SYSTÈMES

Sabotages physiques d'infrastructures

SYSTÈMES

Menaces liées aux drones



AGIR AVANT L'ALERTE

Remis le 21 juillet dernier, le rapport sur la sécurité économique de la France des députés Christophe Plassard (Horizons), Charles Rodwell (Ensemble pour la République) et Jean-Louis Thiériot (Droite républicaine) mettait en évidence que les services d'intelligence économique étaient sollicités trop tardivement et que les entreprises avaient du mal à anticiper les risques. Il recommande aussi d'en sortir par une démarche active, en montrant qu'on se défend, par dissuasion, et en adoptant une logique de recherche d'information dans les contextes concurrentiels. Plus largement, il préconise d'adopter une posture plus offensive en matière de sécurité économique.



LES DANGERS DE L'EXPOSITION INFORMATIONNELLE

Ce qui est public n'a pas besoin d'être volé.

En août 2026, la DGFIP a révélé le vol des données fiscales et cadastrales d'environ 678 000 particuliers et professionnels. L'attaquant s'était connecté à l'aide d'identifiants usurpés, appartenant à un agent et à un tiers habilité. Ce cas rappelle qu'une organisation peut être vulnérable sans que sa protection repose nécessairement sur une faille technique. Une partie du risque se construit en amont, à travers les informations accessibles sur l'organisation, ses collaborateurs et son environnement.

Selon le directeur de la DRSD, 80 % des compromissions dans la sphère défense seraient ainsi liées à de simples négligences (2026). L'enjeu n'est donc pas seulement de protéger ce qui est confidentiel, mais aussi d'identifier ce que l'organisation rend visible et ce qu'un tiers peut en déduire.

CE QU'UNE ENTREPRISE EXPOSE SANS LE SAVOIR

Une information accessible n'est pas nécessairement une information sans valeur. Un organigramme, une offre d'emploi, l'annonce du départ d'un collaborateur, un nouveau fournisseur, un partenariat ou la prise de parole d'un dirigeant peuvent sembler anodins pris isolément. Leur croisement peut pourtant permettre de reconstituer une partie de l'organisation, de ses priorités ou de ses dépendances.

Cette exposition peut également contribuer à faciliter une compromission. Selon Sophos (2026), 79 % des attaques par rançongiciels débuteraient par le vol ou le détournement d'une identité plutôt que par l'exploitation d'une faille technique. Sans réduire la question à la cybersécurité, ce constat illustre l'importance de la dimension humaine : une identité, une fonction ou une information accessible publiquement peut constituer un point d'entrée vers des informations qui ne le sont pas.

Un départ annoncé sur LinkedIn

En annonçant son départ et sa recherche d'opportunités sur LinkedIn, un ingénieur de l'aéronautique a attiré l'attention d'un cabinet étranger de renseignement d'affaires. Selon la DRSD, cette tentative de recrutement a été déjouée. Un signal public peut suffire à identifier une compétence stratégique et à amorcer une démarche de captation de savoir-faire.

Des photos prises sur un salon

À Eurosatory 2026, la DRSD a rappelé les méthodes employées pour collecter des informations sensibles : faux journalistes, repérage des sous-traitants, sollicitations ciblées et tentatives de débauchage. Lors de l'édition précédente, un individu se faisant passer pour un traducteur avait tenté de photographier les composants intérieurs d'un véhicule militaire exposé.

ADOPTER UNE POSTURE OFFENSIVE

Cette exposition informationnelle peut également constituer un levier d'action dans une démarche d'intelligence économique. En amont d'un appel d'offres, d'une opération de M&A ou d'une conquête de marché, le recoupement de sources ouvertes avec des interviews de sources humaines permet de préciser le positionnement des acteurs en présence, d'identifier les décideurs qui pèsent réellement dans la décision, de cartographier les réseaux d'influence et de mieux comprendre les rapports de force. L'enjeu est double : maîtriser les informations que l'on expose, mais aussi tirer parti de celles accessibles sur son environnement pour anticiper les évolutions, éclairer ses décisions et renforcer son avantage concurrentiel.



SENSIBILISER, PAS SEULEMENT PROTÉGER

- Cartographier ce que l'entreprise rend visible publiquement : organigrammes, offres d'emploi, documents indexés, prises de parole de ses dirigeants
- Procéder à une revue systématique des accès lors du départ d'un collaborateur, ou retirer l'accès par défaut lorsqu'un dossier est sensible
- Sensibiliser les collaborateurs présents sur les salons professionnels aux risques de divulgation involontaire d'informations stratégiques lors des échanges avec des tiers
- Avant une opération sensible (M&A, appel d'offres, conquête de marché), mener une enquête approfondie exploitant les informations disponibles en sources ouvertes



L'IA FANTÔME

Quand une entreprise délègue une décision stratégique à un outil d'IA non validé, qui décide réellement à sa place ?

DÉFINITION

L'IA fantôme (ou *Shadow AI*) désigne l'utilisation, par des salariés ou des services, d'outils d'intelligence artificielle générative, de LLM ou d'agents IA autonomes, sans l'approbation ni la connaissance de la direction informatique ou des équipes de sécurité de l'entreprise.

CHIFFRES CLÉS

64%

des salariés admettent utiliser des outils d'IA non autorisés dans leur travail (WatchGuard, 684 salariés de PME et d'ETI, 8 pays dont la France, avril 2026)

75%

des RSSI français jugent que le recours à des services d'IA non approuvés constitue un risque élevé ou très élevé, et ce comportement est cette année celui jugé le plus risqué (baromètre CESIN 2026)

CE QUE ÇA PRÉSENTE COMME RISQUES

- Décision non vérifiée**
Une entreprise ou un salarié peut fonder un choix stratégique sur un rapport généré par IA, sans en connaître les biais ni les limites
- Dépendance sur une fonction critique**
Une activité stratégique, évaluation de partenaires, recrutement, analyse financière, est confiée à un outil que personne dans l'entreprise ne maîtrise vraiment, et dont le fonctionnement reste une boîte noire
- Perte progressive de savoir-faire**
À force de déléguer une tâche à l'IA, l'entreprise risque de perdre la capacité de la faire elle-même
- Fuite de données sensibles**
Les versions grand public de ces outils réutilisent souvent les données saisies pour entraîner leurs modèles
- Perte de maîtrise juridique**
Certaines conditions d'utilisation imposent un stockage des données à l'étranger, sous une loi à portée extraterritoriale
- Surface d'attaque élargie**
Les connexions à des API ou des plugins externes, souvent moins sécurisées, augmentent les risques de fuite ou de compromission

CE QUE LA DGSi A DOCUMENTÉ

Le flash ingénierie de la DGSi (décembre 2025) documente deux cas dans des entreprises françaises stratégiques :



Traduction de documents confidentiels

Dans une entreprise française stratégique, des salariés utilisaient régulièrement, sans l'aval de leur hiérarchie, un outil d'IA générative grand public pour traduire des documents confidentiels. L'entreprise a rapidement demandé de privilégier une solution payante qu'elle avait acquise, et lancé un groupe de travail sur une doctrine d'usage.



Due diligence déléguée à une IA étrangère

Une société française a confié l'évaluation de ses partenaires commerciaux à un outil d'IA créé par une entreprise étrangère. Par manque de temps, elle a suivi systématiquement ses conclusions sans aucune vérification complémentaire.



CE QUE L'ON RECOMMANDE

- Fournir des outils d'IA validés, dans un cadre contractuel qui protège les données
- Ne jamais fonder une décision à enjeu sur un seul rapport généré par IA, sans vérification humaine indépendante
- Vérifier ce que ses sous-traitants et partenaires font des données qu'on leur confie



PANORAMA INSTITUTIONNEL

DGSI

[Flash ingérence](#) - Juin 2026

Trois cas de chercheurs débauchés ou en cumul d'activités non déclaré, avec des transferts de savoir-faire vers l'étranger, parfois détournés à des fins militaires.

[Flash ingérence](#) - Août 2026

Flash spécial sur six modes opératoires de l'ingérence économique étrangère (atteintes capitalistiques, humaines, cybernétiques, physiques, juridiques et à la réputation), illustrés par des cas détectés par la DGSI.

DRSD

[Guide pratique](#) - Septembre 2026

Guide pratique de gestion de la sûreté, qu'elle définit comme la prévention et la lutte contre la malveillance, destiné aux PME et ETI de la base industrielle et technologique de défense.

→ Contre une PME de la défense, une attaque commence souvent par un repérage en ligne et se poursuit par une intrusion physique.

BCE

[Résultats du test de résistance inversé sur les risques géopolitiques](#) - Juillet 2026

Test de résistance inversé : 110 banques ont bâti le scénario géopolitique qui entamerait leur capital, et la BCE les invite à mieux intégrer les risques non financiers, dont les cyberattaques.

→ Pour la BCE, les cyberattaques et les menaces hybrides sont des risques de sécurité, au même titre que les conflits.

ANSSI

[Rapport d'incident](#) - Septembre 2026

Chronologie publique des actes malveillants observés sur le système d'information de la DGFIP entre mai et août 2026.

→ L'ANSSI situe les faiblesses dans trois domaines : l'identité, l'architecture et la détection.

CLUSIF

[Livre blanc "Projets et cybersécurité"](#) - Août 2026

Livre blanc de PMI-France, rédigé avec le Clusif, premier d'une série sur l'intégration de la cybersécurité dans les projets : il traite de l'écosystème et de la gouvernance de la sécurité de l'information.

→ La sécurité et la protection des données se pensent en amont du projet, avec une gouvernance claire des risques numériques.

EN CLAIR

Les attaquants combinent le cyber, l'humain, le physique et le juridique, alors que les défenses restent organisées en silos. Traiter chaque sujet à part, c'est déjà prendre du retard sur la nature réelle de la menace.



Observatoire des Menaces Hybrides

une initiative Consors

// COMPRENDRE POUR AGIR

GARDEZ UNE LONGUEUR D'AVANCE

Chaque trimestre, l'Observatoire décrypte les menaces qui pèsent sur la sécurité de votre entreprise

1 • PRÉVENIR Préparer vos équipes

2 • ANALYSER Comprendre votre exposition

3 • AGIR Répondre à une attaque

Suivez-nous pour ne manquer aucune édition