MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Lettre d'information économique
N°20 – Juillet 2025

Panorama des ingérences à l'encontre de la sphère de Défense en 2024

LE MOT DU DIRECTEUR

Mesdames, Messieurs,

Comme en 2023, l'année 2024 a été marquée par un contexte géopolitique international particulièrement instable, durci notamment par la poursuite des affrontements à l'est de l'Europe, un accroissement des tensions au Proche-Orient et le renforcement des convoitises de nos principaux compétiteurs stratégiques à l'égard de notre potentiel de Défense.

Dans de telles circonstances, les agents de la DRSD s'attachent à garantir la sécurité et l'intégrité de l'ensemble de l'écosystème industriel de Défense par leur mission de détection et d'entrave aux tentatives d'ingérences économiques.

Ainsi, l'année 2024 s'est caractérisée par un nombre élevé et constant d'atteintes à l'encontre des entreprises de notre base industrielle et technologique de Défense (BITD). La diversité de ces ingérences, telles que décrites dans ce numéro de la *Lettre d'information économique* (LIE), accroît la nécessité de poursuivre nos actions au profit de l'ensemble des acteurs économiques et industriels qui concourent à la Défense nationale.

Afin de vous présenter les principaux secteurs visés et les modes opératoires susceptibles d'être utilisés à votre encontre, cette LIE vous présente un état de la menace établi à partir des remontées d'informations que vous avez adressées à la DRSD en 2024. Illustré de cas concrets et de recommandations pratiques, ce numéro a pour ambitions de vous aider à renforcer votre politique de sécurité et de vous accompagner dans la réduction et la maîtrise des risques à l'encontre de vos entités.

Demeurez assurés que mes agents restent mobilisés pour vous accompagner dans la protection de votre personnel, de vos informations sensibles, de vos savoir-faire et de vos infrastructures.

Général de corps d'armée Philippe Susnjara
Directeur du Renseignement et de la Sécurité de la Défense

SOMMAIRE

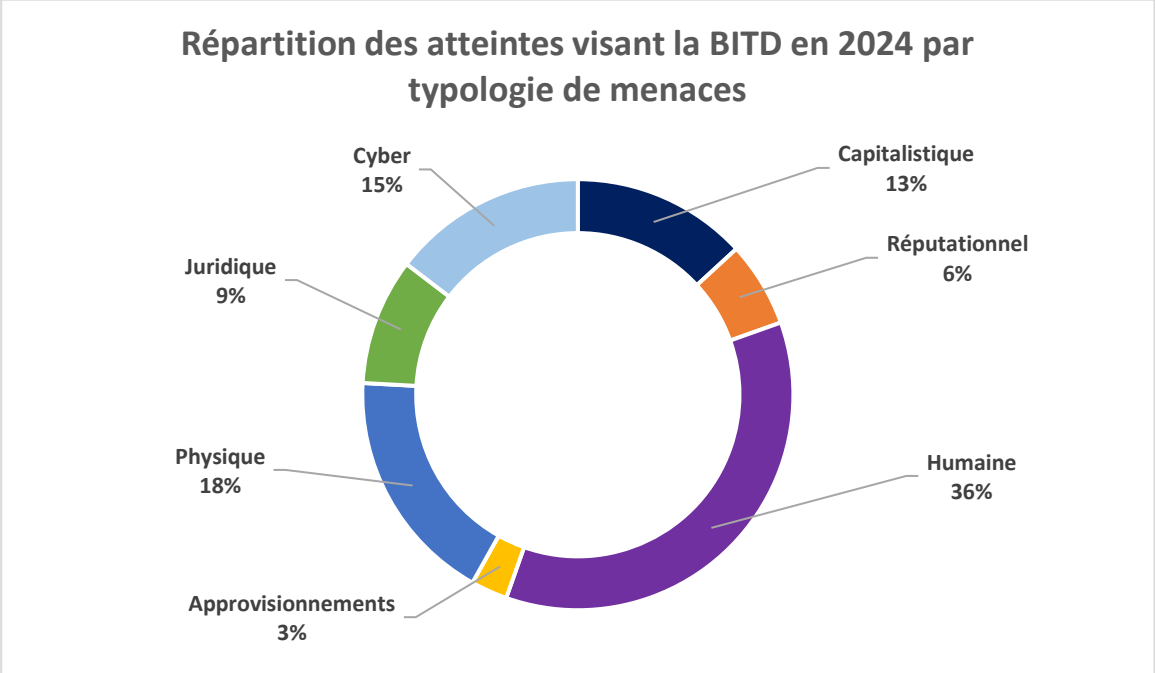
LES ATTEINTES À LA BITD RECENSÉES PAR LA DRSD EN 2024

Le Service a décelé, en 2024, un nombre élevé d'ingérences à l'encontre de la BITD. Néanmoins stable par rapport aux chiffres de 2023, ce bilan confirme une tendance de fond observée sur les dernières années.

À ce titre, le Service relève que la menace sur les approvisionnements en matières premières critiques (terres rares, semi-conducteurs, etc.) et en outils de production reste constante. Concernant l'espionnage industriel, commercial et technologique, la DRSD observe une persistance des ingérences qui reposent sur des modes d'action de plus en plus décomplexés (vols d'informations et de supports numériques, prédation capitalistique, ingérences juridiques, etc.). Ces ingérences portent aussi bien sur les savoir-faire industriels que sur les avancées scientifiques et techniques ou encore sur les expertises technologiques nationales.

Alors que tous les secteurs de la BITD peuvent être concernés par ces atteintes, le Service a observé un ciblage accru des secteurs aéronautique et spatial en 2024. Par ailleurs, les technologies de rupture, à l'image du quantique ou de l'intelligence artificielle, continuent de faire l'objet de convoitises de la part de nombreux pays. Outre cette menace constante, le Service a détecté une hausse des atteintes dans les secteurs des drones et de la maîtrise des fonds marins, secteurs pour lesquels la France possède un avantage concurrentiel certain.

Cette année encore, la DRSD constate que le vecteur humain demeure prépondérant, avec toutefois une forte croissance du nombre d'incidents cyber signalés, qui ont doublé depuis 2023.



1. LE VECTEUR HUMAIN : PRINCIPALE MENACE D'INGÉRENCES

Le nombre d'atteintes dites « humaines » (chantage, faux entretiens de recrutement, vols d'ordinateurs, tentatives de débauchage, etc.) n'a cessé de **croître** ces dernières années. Cette tendance se confirme en 2024 (36 % des atteintes) bien qu'en proportion plus faible par rapport à l'année 2023 (45 %).

Certains compétiteurs étatiques mettent ainsi en œuvre des stratégies complexes d'acquisition de savoir-faire *via* des débauchages ciblés ou l'envoi d'étudiants dans des laboratoires et programmes de recherche sensibles.

La Chine privilégie plus particulièrement ces modes d'actions afin de cibler les **centres de recherche liés à la sphère de Défense et les marchés des technologies de l'information et de la communication, tous porteurs d'innovations**.

Sur les marchés européens, les compétiteurs de la BITD française ont recours à des stratégies de débauchage ciblé de collaborateurs experts, particulièrement dans les secteurs de l'aéronautique, du spatial et des véhicules terrestres.

Cas concret

Tentative de débauchage chinois au sein d'une entreprise spécialisée dans l'aéronautique

Au début de l'année 2024, un collaborateur chinois qui avait quitté une entreprise spécialisée dans l'aéronautique a repris attache avec un ancien collègue toujours en poste pour que ce dernier identifie puis lui communique les noms de spécialistes au sein de cette structure. La contrepartie de ce « service » était une proposition de poste en Chine à des conditions financières avantageuses. Lorsqu'elle a été alertée, la chaine *Sûreté* de l'entreprise, qui avait déjà bénéficié d'une sensibilisation du Service, a demandé au collaborateur contacté de ne plus répondre aux sollicitations de son ancien collègue.

Cette manœuvre illustre une tentative de débauchage ciblé en vue d'une captation de savoirs et savoir-faire qui menace la BITD française. D'une manière plus générale, ce risque est considéré comme élevé.

2. LA RECRUDESCENCE DES ATTEINTES PHYSIQUES

Au cours de l'année 2024, la menace physique (intrusions, dégradations d'enceinte/sabotages, surveillances de sites) a **augmenté** à l'encontre des entreprises de la BITD. Les **intrusions**, avérées comme suspectées, et les tentatives avortées représentent cette année encore **plus de la moitié des incidents physiques détectés** auprès des entreprises de la BITD.

Depuis fin 2023, **plusieurs actions d'origine criminelle** ont ciblé des entreprises de Défense. Ces atteintes prennent principalement la forme d'incendies qui ciblent les infrastructures énergétiques des sociétés.

Dans ce cadre, les actions contestataires de la mouvance d'ultragauche (UG) ont continué de s'intensifier.

Cas concret

Sabotages à l'encontre d'une entreprise de Défense

Au cours du premier trimestre 2024, une société qui produit des drones a été la victime des conséquences d'un incendie criminel du transformateur électrique situé à proximité immédiate de son emprise et qui alimente ses lignes de production.

Cet incident s'est traduit par la mise à l'arrêt de la chaîne de production pendant plusieurs heures.

Au-delà du préjudice économique immédiat, de tels incidents peuvent avoir des conséquences financières durables, en raison de l'arrêt de la production qui en découle.

Dans les jours qui ont suivi les faits, les dégradations ont été revendiquées par des groupes liés à la mouvance UG.

3. L'AUGMENTATION SIGNIFICATIVE DES ATTAQUES CYBER

En 2024, les attaques cybernétiques ont **augmenté de moitié** par rapport à l'année précédente. Elles sont, dans leur grande majorité, perpétrées par l'**écosystème cybercriminel** qui a conservé ses vecteurs d'infection classiques[1] pour pénétrer les systèmes d'information de ses cibles dans l'industrie de Défense.

Comme en 2023, ces groupes ont cherché à porter atteinte aux sites internet institutionnels des sociétés françaises impliquées dans la fourniture d'armes aux forces armées ukrainiennes. Au cours de l'année 2024, ces attaques ont porté atteinte en particulier aux secteurs de **l'aéronautique** et des **nouvelles technologies de l'information et de la communication**.

Malgré la hausse des atteintes cybernétiques, le Service a observé que le personnel de la BITD apparaît davantage sensibilisé aux tentatives dites d'« hameçonnage »[2]. Les efforts en la matière doivent donc être poursuivis.

Cas concret

Attaque cyber visant une société de Défense exportant vers l'Ukraine

Après l'annonce de ses livraisons de matériel militaire à l'Ukraine, une société de défense française a fait part à la DRSD de difficultés rencontrées dans la gestion de ses systèmes d'information.

En effet, quelques jours après la communication de sa participation au soutien à l'Ukraine, l'entreprise a été la cible d'attaques par déni de service (DDoS), qui ont momentanément paralysé ses systèmes d'information.

Comme elle avait anticipé ce type d'atteintes, les actions malveillantes n'ont pas eu de conséquence sur l'activité de l'entreprise.

[1] Hameçonnage, rançongiciel, attaques par déni de service (DDoS : *Distributed Denial of Service*. Attaque visant à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer ou par l'exploitation d'une faille de sécurité pour provoquer une panne ou un fonctionnement fortement dégradé).

[2] L'hameçonnage, ou *phishing* en anglais, est une technique frauduleuse destinée à leurrer un utilisateur pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passes, etc.) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique, d'une banque, d'un réseau social, d'un opérateur de téléphonie, d'un fournisseur d'énergie, de site de commerce en ligne, d'administrations publiques ou d'entreprises.

4. LE RISQUE ACCRU DE PRÉDATION CAPITALISTIQUE SUR NOS SAVOIR-FAIRE

Nation la plus attractive d'Europe en matière d'investissements pour la sixième année consécutive[3], la France a accueilli plus de 1 800 projets d'investissements étrangers en 2024 qui contribuent à soutenir la croissance, l'innovation et l'emploi dans le pays. Dans un contexte de décélération de la croissance mondiale et de fortes tensions géopolitiques, l'investissement en France se montre particulièrement résilient.

Pour autant, la vigilance reste nécessaire pour se prémunir de certains investissements étrangers prédateurs, motivés par la captation de savoirs et savoir-faire propres aux capacités industrielles de Défense française. Pour s'adapter aux éventuelles stratégies de contournement, l'État continue de renforcer sa procédure de contrôle des investissements étrangers[4]. Ainsi, la France a **notamment étendu les secteurs stratégiques couverts par la procédure et les acteurs qui relèvent de son contrôle**. Les prises de contrôle de succursales d'entités de droit étranger et qui exercent une activité sensible font désormais partie des opérations financières surveillées. Dans cette perspective, si l'arrivée d'investisseurs étrangers constitue une opportunité pour l'entreprise, elle représente un risque dès lors qu'elle favorise l'adoption d'orientations contraires aux intérêts français. De manière factuelle, les **États-Unis demeurent en France les premiers investisseurs** dans le secteur de la Défense. Les secteurs concernés sont ceux particulièrement innovants des semi-conducteurs, de l'intelligence artificielle et d'autres technologies stratégiques. Ce constat impose un contrôle accru du ministère de l'Économie et des Finances, accompagné par les autres services de l'État, afin de se prémunir d'éventuelles captations de savoirs et savoir-faire.

Cas concret

Rachat étranger d'une société française de Défense par un actionnaire lié à un investisseur récemment entré dans le capital

En 2024, la mise en vente d'une entreprise spécialisée dans l'optronique a suscité l'intérêt d'investisseurs étrangers. **L'un des investisseurs de la société, récemment entré au capital et de nationalité étrangère, a appuyé une offre de rachat issue de son pays d'origine.**

Ainsi, **la vulnérabilité financière d'une entreprise et le tropisme d'un de ses investisseurs** peuvent faire courir le risque d'une ingérence capitalistique **(fuite d'informations sensibles et captation de savoir-faire)**. Pour en limiter la portée, l'entreprise peut être accompagnée par les différents services de l'État impliqués dans le contrôle des investissements étrangers en France (IEF) à travers la sensibilisation à la prédation capitalistique, l'identification d'autres investisseurs nationaux, le soutien à l'activité au moyen de fonds spécialisés (ex : Bpifrance), etc.

En effet, l'arrivée d'actionnaires étrangers au capital d'une entreprise française peut nuire à son appareil industriel et à sa compétitivité : déstabilisation de la gouvernance, évolution de la stratégie commerciale, pertes de savoir-faire voire cession d'actifs stratégiques au détriment des intérêts de la Défense nationale.

[3] Source : Business France.

[4] Contrôle des investissements étrangers en France (IEF) : l'article L. 151-3 du Code monétaire et financier soumet les investissements étrangers à une procédure d'autorisation préalable, dans des secteurs limitativement énumérés, touchant à la défense nationale ou susceptibles de mettre en jeu l'ordre public et les activités essentielles à la garantie des intérêts du pays (source : Direction générale du Trésor).

5. L'USAGE DU DROIT À DES FINS STRATÉGIQUES

Les **États-Unis** et la **Chine** demeurent les deux principaux acteurs en matière d'utilisation de **leurs dispositifs juridiques à des fins stratégiques (*lawfare*)**. Or, ils s'appliquent dès lors qu'un lien avec ces deux pays est établi (fournisseur, filiale, etc.), ce qui peut être évité en mettant en œuvre, dès leur conception, des programmes d'équipements dits « ITAR *free* »[5].

Le recours au *lawfare* par les autorités américaines se traduit notamment par des dispositions législatives et réglementaires à portée extraterritoriale qui **contraignent l'activité des entreprises françaises**. Par ailleurs, les autorités américaines ont également souhaité renforcer leur influence au sein des **instances internationales de normalisation**.

Si le risque d'ingérence par l'application de dispositifs législatifs et réglementaires chinois à portée extraterritoriale reste à ce stade **modéré**, des difficultés d'approvisionnement et l'adoption de mesures de rétorsion à l'encontre des entreprises françaises ne peuvent être écartées. Ainsi, le Service a observé l'an passé les premières **difficultés d'approvisionnement** liées au **contrôle de l'exportation du germanium** par l'administration chinoise.

Cas concret

Audit américain exposant une société de l'aéronautique à des fuites d'informations

Au premier semestre 2024, une société française de l'aéronautique a fait l'objet d'un audit de l'administration américaine afin d'évaluer sa conformité aux réglementations américaines de contrôle des exportations.

À ce titre, l'entreprise a été accompagnée par le Service en vue de limiter le risque de fuite ou de captation d'informations sensibles par un cabinet d'audit externe ou un représentant de l'administration américaine.

L'usage de l'arsenal juridique américain à portée extraterritoriale constitue une menace omniprésente et contraignante pour l'activité des entreprises de Défense qu'il s'agit de considérer dans les prospects.

[5] Cf. instruction 1618 de la Direction générale de l'armement (DGA) relative au déroulement des opérations d'armement.

6. LE DURCISSEMENT DE LA MENACE RÉPUTATIONNELLE

En 2024, les attaques des mouvances antimilitaristes et pro-palestiniennes se sont **intensifiées**. Les modes opératoires auxquels ont recours les activistes antimilitaristes ou anarchistes révèlent des **organisations et des capacités de ciblage toujours plus structurées**.

Le conflit israélo-palestinien et le lien commercial entre des entreprises françaises et l'État israélien a motivé l'organisation de plusieurs **manifestations pro-palestiniennes** aux abords d'entreprises de Défense ou de salons d'armement. D'autres manœuvres, notamment sur le plan juridique, qui visaient à mettre la pression sur les acteurs de la Défense ont été relevées.

Dans ce contexte, il est essentiel de se conformer aux règlementations en vigueur en matière de contrôle des exportations et de *due diligence*[6].

Cas concret

Manifestation pro-palestinienne devant les locaux d'une société qui exporte du matériel militaire vers Israël

Au court de de l'année 2024, un groupe pro-palestinien a manifesté à plusieurs reprises devant une société de Défense française qui livre du matériel militaire à une entreprise israélienne.

Cette action constitue une **atteinte réputationnelle** qui peut s'inscrire dans une campagne d'attaque plus globale, notamment en combinant plusieurs vecteurs. Elle peut nuire à l'activité économique de la société ciblée.

D'autres modes opératoires ont été observés, à l'image de **campagnes numériques de dénigrement** des entreprises de la BITD ou des **pressions** exercées à l'encontre de sociétés qui participaient à des salons de Défense.

[6] Voir la LIE n°12 – *La contre-ingérence dans le contrôle des exportations de matériels de guerre* d'avril 2023

GARDONS LE CONTACT

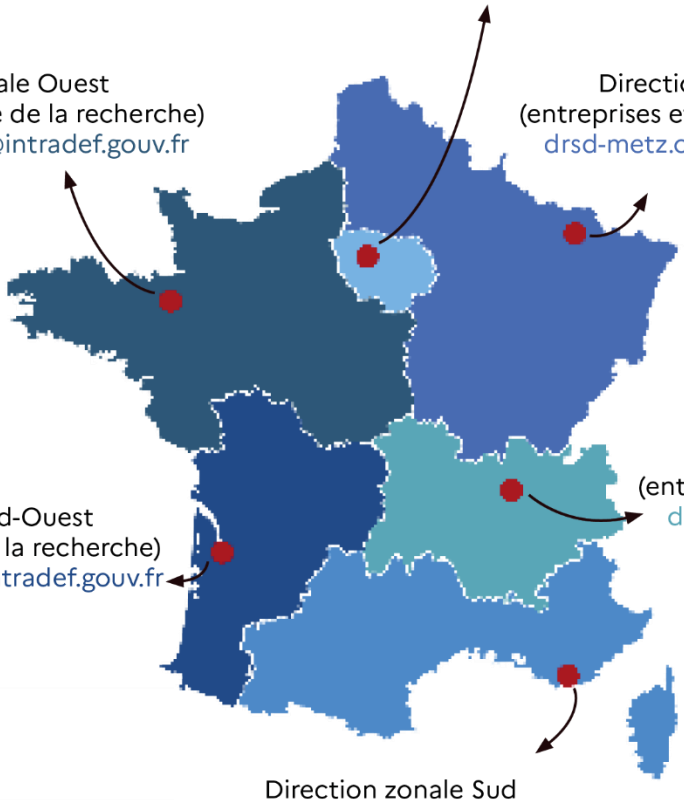
Direction centrale
Section Sensibilisation
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Direction zonale Hors métropole
drsd-dzhm.cmi.fct@intradef.gouv.fr

Direction zonale Ile-de-France
Entreprises : drsd-dsezp-4.cds.fct@intradef.gouv.fr
Écoles et instituts de recherche : prsd-villacoublay.cmi.fct@intradef.gouv.fr

Direction zonale Ouest
(entreprises et monde de la recherche)
drsd-rennes.cmi.fct@intradef.gouv.fr

Direction zonale Nord-Est
(entreprises et monde de la recherche)
drsd-metz.cmi.fct@intradef.gouv.fr



Direction zonale Sud-Est
(entreprises et monde de la recherche)
drsd-lyon.cmi.fct@intradef.gouv.fr

Direction zonale Sud-Ouest
(entreprises et monde de la recherche)
drsd-bordeaux.cmi.fct@intradef.gouv.fr

Directions zonales (DZ)

Direction zonale Sud
(entreprises et monde de la recherche)
drsd-toulon.cmi.fct@intradef.gouv.fr

CERT [ED]

0 805 046 300*

*Appel gratuit

cert-drsd.contact.fct [@] def.gouv.fr

Suivez-nous sur les réseaux sociaux et sur notre site internet
www.defense.gouv.fr/drsd