LIE n°16 de la DRSD

Panorama des ingérences à l'encontre de la sphère défense en 2023

La lettre d'information économique
Juillet 2024

Sommaire

Éditorial du Directeur du Renseignement et de la Sécurité de la Défense

Mesdames, Messieurs,

L'année 2023 aura été marquée par le durcissement du contexte géopolitique international, illustré notamment par la permanence de l'affrontement aux frontières orientales de l'Europe, l'émergence subite d'un conflit aux impacts étendus bien au-delà du Moyen-Orient et la hausse de tensions latentes ou incarnées entre puissances. Pour la sphère de défense, dont la protection est la raison d'être de la DRSD, ces événements et états de crise auront eu pour effet induit ou direct une recrudescence des actions d'ingérences visant à porter atteinte au potentiel et aux intérêts de la défense nationale.

Ainsi, en 2023, l'ensemble des acteurs stratégiques de la défense, la base industrielle et technologique de défense (BITD) en premier lieu, ont dû faire face aux convoitises croissantes de la part de nos compétiteurs internationaux.

Ces multiples actes d'ingérences ont nécessité de la part de tous le renforcement des mesures de vigilance, en particulier face aux menaces d'espionnage, de sabotage, d'atteintes réputationnelles, étendues à d'autres modes de déstabilisation décrits dans ce numéro de la Lettre d'Information Economique (LIE).

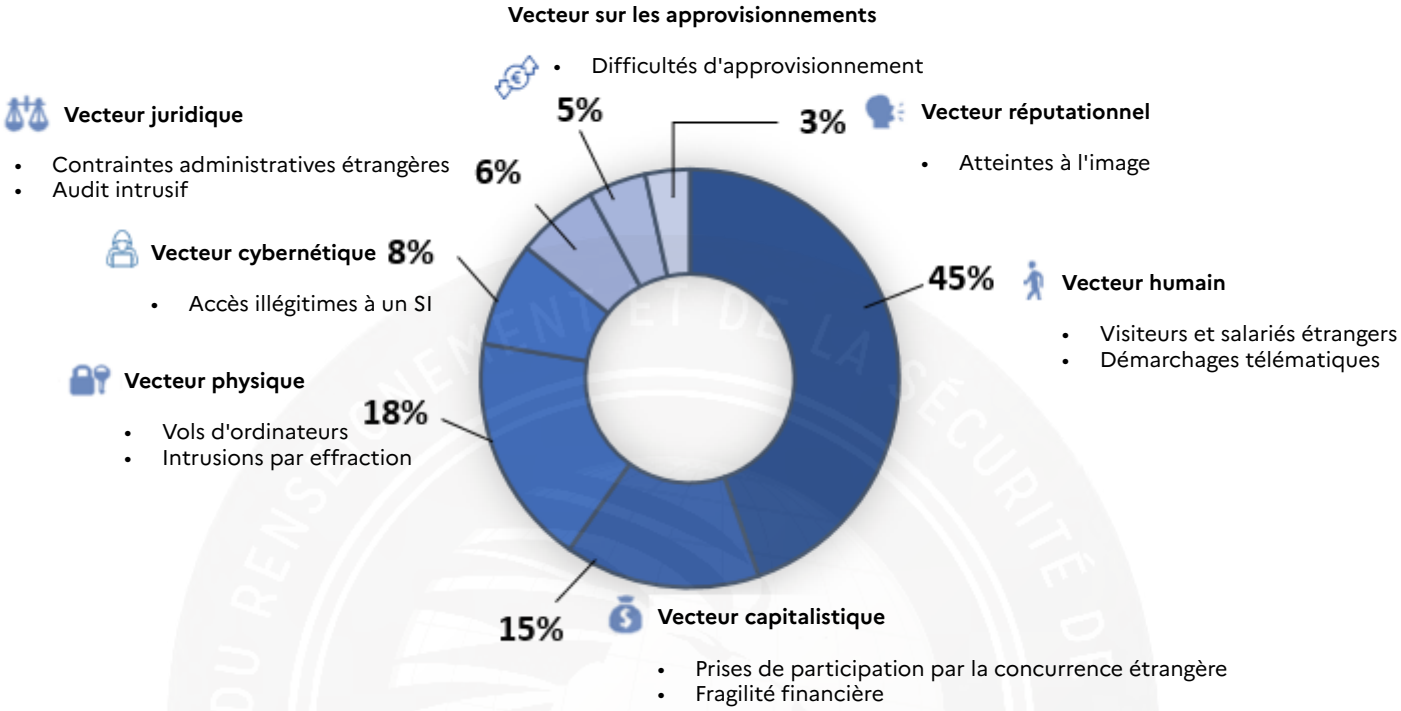
Afin de vous accompagner dans la réduction et la maîtrise de vos risques, cette LIE vise à présenter un état de la menace pesant sur l'écosystème de la défense (principaux modes opératoires, acteurs ingérents et secteurs convoités), pour vous permettre d'enrichir votre stratégie de sécurité, au travers de différents cas-concrets et de recommandations adaptées.

Lorsque la crise se dessine et s'impose, il importe de serrer les rangs pour s'y préparer puis pour l'affronter. Soyez une fois de plus assurés que nos agents restent plus que jamais mobilisés pour conseiller et accompagner le renforcement de vos processus de sécurité afin de préserver vos collaborateurs, vos informations ainsi que le patrimoine matériel et immatériel de vos entreprises, préalable obligatoire à l'accroissement de nos capacités de production nationales, de notre souveraineté nationale et de l'expression de notre puissance.

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

Menace humaine : en nette progression

Vecteurs d'ingérences en 2023



Le nombre d'atteintes dites « *humaines* » (chantage, faux entretiens de recrutement, vols d'ordinateurs, stratégies de débauchage, etc.) visant l'industrie de défense et la recherche d'intérêt défense continue de **croître** en 2023.

Certains collaborateurs, dirigeants, ingénieurs ou agents commerciaux, notamment à l'occasion de déplacements professionnels à l'étranger, ont subi des tentatives de chantage reposant sur des infractions, réelles ou supposées, à la législation nationale afin d'obtenir de leur part des informations sensibles sur leur entreprise.

En parallèle de ce mode opératoire, certaines nations et sociétés concurrentes mettent en place de véritable stratégies de débauchage visant à capter, notamment à l'occasion de voyages d'affaires, le savoir-faire et les connaissances des collaborateurs d'entreprises françaises. Ces modes opératoires peuvent être précédés d'approches par le biais de faux entretiens de recrutement, qui se sont multipliées en 2023 à la faveur de l'expansion constante de l'usage des réseaux sociaux.

Enfin, les vols d'ordinateurs, en augmentation, continuent de représenter un risque majeur de captation de données d'intérêt commercial pour les entreprises de défense et leurs collaborateurs, tant pendant leurs activités professionnelles qu'extra-professionnelles.

Ces modes opératoires s'inscrivent au cœur de stratégies souvent plus larges d'influence, de lobbying et d'entrisme, fréquemment employées par certains états offensifs.

CAS CONCRET : CAMPAGNE CHINOISE DE CIBLAGE DE CHERCHEURS FRANÇAIS

Depuis novembre 2022, un cabinet de conseil chinois mène une **campagne massive de débauchages** dans le milieu de la recherche scientifique française. Dans ce cadre, les structures de recherche contribuant à la défense sont particulièrement ciblées. Le Service a ainsi pu confirmer que plus de 650 approches échelonnées ont été identifiées au cours de l'année 2023.

Menace capitalistique : une attention spécifique portée aux investissements étrangers

Nation la plus attractive d'Europe pour la cinquième année consécutive, la France a accueilli plus de 10 000 projets d'investissements étrangers entre 2017 et 2023, contribuant à soutenir la croissance, l'innovation et l'emploi dans le pays.

Lorsque ces investissements visent des secteurs jugés « sensibles », l'État dispose d'une procédure d'autorisation préalable à laquelle doivent se soumettre les investisseurs étrangers, de manière à assurer le maintien des savoirs et des savoir-faire de nos entreprises et faire obstacle à leur captation.

Premiers investisseurs dans la BITD française, les États-Unis investissent prioritairement dans les domaines des nouvelles technologies, des semi-conducteurs, de l'intelligence artificielle et du quantique, secteurs particulièrement stratégiques qui justifient un contrôle accru du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique, accompagnés par les autres services de l'État.

Par ailleurs, la Chine qui investit en France dans les secteurs sensibles de l'industrie, l'énergie, la santé, l'électronique et les télécommunications, **contourne parfois les restrictions croissantes imposées par la législation française aux investisseurs étrangers**[1] en utilisant des sociétés chinoises qui procèdent à des investissements **sous le seuil de déclenchement du contrôle IEF**[2].

CAS CONCRET : REFUS DE LA DEMANDE D'IEF DÉPOSÉE PAR UN GROUPE AMÉRICAIN SUR DES SOCIÉTÉS STRATÉGIQUES FRANÇAISES ET CANADIENNES

Dans le cadre d'une demande d'IEF déposée par un groupe américain pour l'acquisition d'un fabricant canadien de robinetterie industrielle et de ses filiales françaises, le ministre de l'Économie, des Finances et de la Souveraineté industrielle et numérique a refusé cet investissement. Cette décision fut motivée par la criticité des prestations fournies par ces filiales pour les secteurs nucléaires civil et militaire français et des risques liés à la nationalité américaine de l'investisseur.

[1] 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).

[2] 10% du capital pour les sociétés cotées / 25% pour les sociétés non-cotées.

Menace physique : augmentation des atteintes à l'encontre des emprises industrielles

En 2023, le nombre d'incidents de sécurité à l'encontre des emprises de l'industrie de défense a augmenté d'environ 10% par rapport à l'année précédente.

Les intrusions (avérées, tentées ou suspectées) représentent plus de 60% des incidents constatés au sein de la BITD, suivies des repérages, des survols de drones et des détériorations d'enceintes. Quel que soit le mode opératoire choisi, de l'intrusion « en force » (ex. franchissement de clôture de nuit) ou « par ruse » (ex. usage d'une fausse qualité), le caractère malveillant est établi pour un certain nombre de ces intrusions qui ont occasionné le vol de matériels informatiques ou de matériaux, mais également le déclenchement d'incendies volontaires, dont la motivation s'est avérée criminelle, contestataire ou relevant d'une volonté de sabotage.

Les différents appels à dénoncer et entraver les ventes d'armement français sur fond de conflits en Europe de l'Est comme au Moyen-Orient, pourraient se traduire dans les prochains mois par des actions plus ciblées (manifestations, envahissement de sites, sabotages, etc.). À cet effet, l'exposition médiatique de certains sites doit faire l'objet d'une attention toute particulière et d'une parfaite maîtrise, tant il est vrai qu'elle peut attirer l'attention de certains acteurs malveillants.

CAS CONCRET : INTRUSION « CONSENTIE » LORS DE TRAVAUX SUR UN SITE

Dans le cadre de travaux de rénovation, une entreprise de la défense contractualise avec une société spécialisée afin de réaliser une intervention sur un site industriel sensible.

Bien que les travaux n'aient aucune conséquence sur l'activité du site, les employés de la société doivent accéder à l'emprise durant une semaine.

À leur arrivée sur le site, les employés se présentent au poste de filtrage et leur identité est contrôlée. Après vérification, la sécurité de l'emprise se rend compte qu'un des employés étrangers présente une fausse carte d'identité bulgare. En réalité, l'individu est ressortissant d'un autre pays, proche de la Bulgarie, et se trouve de manière illégale sur le territoire national.

L'intéressé est alors invité à patienter dans une salle d'attente, le temps pour les responsables sécurité de prévenir les forces de sécurité intérieure pour procéder à son interpellation.

La vigilance de la chaîne de sécurité a ainsi permis d'empêcher qu'un ressortissant d'un pays de la sphère d'influence russe, en situation irrégulière, soit autorisé à pénétrer sur une emprise sensible.

Menace physique : augmentation des atteintes à l'encontre des emprises industrielles

Principales recommandations

- ☐ Établir et vérifier préalablement la liste des personnes devant accéder à votre établissement ;
- ☐ Prévoir des badges dédiés à la présence de ces personnes (ex. badges visiteurs identifiables sans ambiguïté par un code couleur) ;
- ☐ Organiser préalablement une réunion entre la chaîne de sécurité et le personnel encadrant des sociétés prestataires, pour aborder les sujets de sécurité (règles à respecter, remontées d'incidents, etc.) ;
- ☐ Sensibiliser le personnel au signalement de toute situation anormale (regroupements en périphérie du site, comportement douteux, etc.) à la chaîne de sécurité, qui en tiendra informée la DRSD et les autres services en charge de la sécurité.

FOCUS. Recrudescence des survols de drones

En 2022, on estimait à 3 000 000 le volume de drones en circulation en France. Leur présence dans l'espace aérien augmente sans cesse. Dès lors, chaque site peut faire l'objet d'un survol, mal intentionné ou fortuit. Au regard des menaces qu'il peut engendrer (du simple accident à la captation d'informations sensibles par exemple), chaque survol doit être considéré comme un événement particulier qui doit être pris en compte.

Cela passe par :

- La sensibilisation de votre personnel à sa propre sécurité et à celle des activités, en privilégiant la mise à l'abri de chacun en cas de survol ;
- Le signalement en temps réel des faits aux forces de sécurité intérieure (Gendarmerie et Police), seules habilitées à intervenir contre le vecteur et son télépilote ;
- La systématisation du rapport de ce type d'évènement à votre responsable de la sécurité et à votre correspondant DRSD.

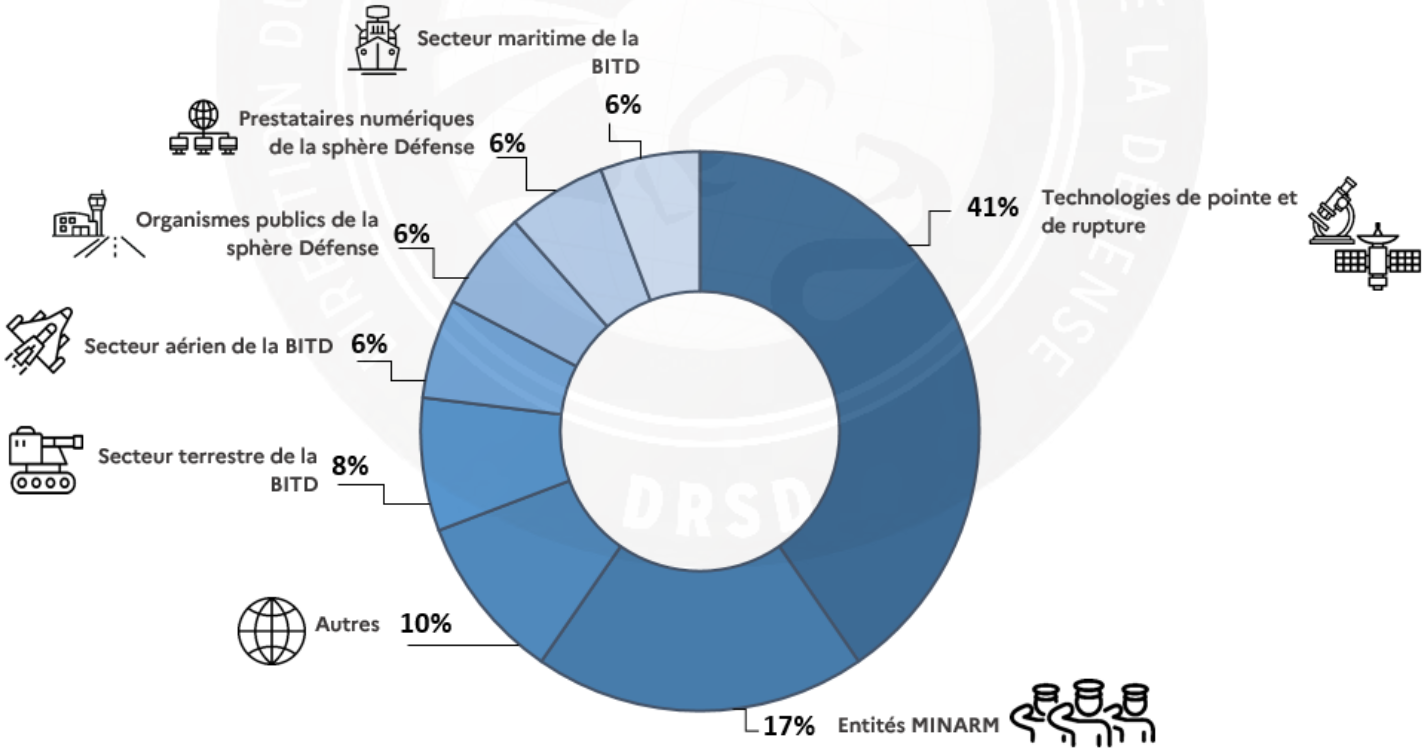
Menace cyber : émergence de nouveaux acteurs

En 2023, le nombre d'attaques à but lucratif, principalement issues de l'écosystème cybercriminel russophone, reste la principale menace pour la BITD. L'attaque par force brute[3] et l'hameçonnage sont les vecteurs d'infection les plus observés par le Service. Après être parvenu à pénétrer dans le système d'information de la victime, l'attaquant vise de plus en plus à récupérer une partie ou l'ensemble des données de la société afin de procéder à des manœuvres de rançonnage, voire à les revendre en ligne sur le *dark web*.

Au sein de cet écosystème cybercriminel, de nouveaux acteurs nourrissant des intentions plus idéologiques se sont imposés. Ainsi, des cyber-activistes pro-russes, très réactifs à l'actualité, revendiquent régulièrement des attaques par DDoS[4] visant en particulier à porter atteinte à la réputation ou à l'activité des sociétés directement impliquées dans le soutien militaire français à l'Ukraine.

Par ailleurs, les groupes étatiques de type APT[5], disposant de capacités techniques plus avancées, constituent une menace prégnante. Leurs attaques ont pour principale finalité l'espionnage industriel et l'atteinte aux capacités de production des sociétés ciblées.

Concernant les victimes, le Service observe que les entreprises des industries de pointe (domaines spatial et aéronautique), ont été particulièrement touchées l'an passé.



[3] Attaque informatique consistant à tester chaque combinaison possible d'un mot de passe ou d'une clé pour un identifiant donné afin de se connecter au service ciblé.

[4] *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.

[5] Cyberattaque sophistiquée et ciblée de longue durée menée par un groupe disposant de compétences techniques avancées, souvent supposé associé ou soutenu par un Etat. Le terme APT désigne indifféremment l'attaque et le groupe menant l'attaque.

Menace cyber : émergence de nouveaux acteurs

CAS CONCRET : REVENDICATION DE FUITE DE DONNÉES CONTRE UNE ENTREPRISE DE LA BITD

Un groupe de cyber attaquants, procédant par rançongiciel, revendique une exfiltration de données à l'encontre d'une entreprise de la BITD soutenant l'effort de guerre ukrainien. Cette nouvelle bénéficie d'un fort impact médiatique et nuit directement à la réputation de l'entreprise. Cette dernière met en œuvre une cellule de crise pour identifier la brèche dans l'un de ses systèmes et l'origine de la fuite. En parallèle, elle met en place une communication de crise en interne ainsi qu'auprès de ses clients.

Après enquête, il s'avère qu'il s'agissait d'un agrégat de données exfiltré chez un prestataire, ce qui souligne le besoin de s'assurer également de la qualité du niveau de protection des SI des sous-traitants.

Principales recommandations

- ☐ Mettre à jour régulièrement vos SI, votre solution antivirus et vos applications de travail ;
- ☐ Sensibiliser régulièrement votre personnel sur l'importance de son rôle dans la remontée d'informations auprès des RSSI et/ou de la chaîne de sécurité ;
- ☐ Communiquer régulièrement à vos collaborateurs (par affichage, messagerie interne, etc.) les bonnes pratiques d'usage de leurs outils numériques, aussi bien professionnels que personnels.

Pour ce faire, vous pouvez notamment utiliser la documentation disponible sur les sites de l'ANSSI et Cybermalveillance.

Menace juridique : usage décomplexé du droit à des fins stratégiques (*lawfare*)

Certains compétiteurs tels que les **États-Unis** et la **Chine** ont régulièrement recours à l'instrumentalisation de leurs dispositifs juridiques à des fins concurrentielles, avec un renforcement de l'**application de leurs lois extraterritoriales,** contraignant l'activité des entreprises françaises et la mise en œuvre de **stratégies offensives** au sein des instances internationales de normalisation.

Les États-Unis ont continué d'entretenir une application contraignante de certains de leurs dispositifs à l'égard de la BITD, en s'appuyant notamment sur la vérification de la conformité d'entreprises aux réglementations relatives au contrôle export (ITAR[6] et EAR[7]), y compris sur le territoire national.

Quelques années après l'adoption par la **Chine** d'une série de législations à portée extraterritoriale, le Service a relevé leurs **premiers effets** sur l'activité des entreprises de la BITD. Bien que le risque d'ingérence, par l'application directe des dispositifs législatifs et réglementaires chinois soit à ce stade modéré, des difficultés d'approvisionnement ou l'adoption de mesures de rétorsion à l'encontre des entreprises françaises ne peuvent être écartées.

CAS CONCRET : EXPOSITION D'UNE SOCIÉTÉ FRANÇAISE DE LA BITD À DE POTENTIELLES SANCTIONS AU MOTIF DE RELATIONS COMMERCIALES AVEC LA CHINE

Au cours de l'année 2023, une entreprise française de la BITD a identifié des irrégularités dans ses exportations de produits d'origine américaine vers des clients chinois. En effet, la réexportation de certains composants américains vers la Chine est désormais soumise à des contrôles accrus, depuis l'adoption de la *Military End User List* (MEU) en 2020 et la réglementation du 7 octobre 2022[8].

Ainsi, l'entreprise française pourrait à la fois être exposée à des sanctions administratives américaines si ces irrégularités sont avérées, ainsi qu'à de potentielles mesures de rétorsion commerciales de la part du gouvernement chinois en cas d'interruption des livraisons concernées.

[6] ITAR : *International Traffic in Arms Regulations*

[7] EAR : *Export Administration Regulations*

[8] Les réglementations adoptées par le Bureau of Industry and Security (BIS) le 07/10/2022 ont été mises à jour le 17.10.2023.

Menace juridique : risque accru d'atteintes au contrôle des exportations

Depuis le déclenchement du conflit russo-ukrainien en 2022, les risques de détournement de biens à double usage (civil et militaire) et de dissémination de matériels de guerre se sont amplifiés. En effet, les sociétés françaises se trouvent de plus en plus sollicitées par des intermédiaires ou des sociétés jusqu'alors « inconnus », au sujet desquels elles ne disposent d'aucun élément permettant de vérifier l'honorabilité afin de contracter des biens ou des services pouvant être employés en tant que matériels de guerre. Ces approches peuvent être en réalité destinées à alimenter des pays sensibles, sous sanctions, proliférants ou qualifiés de « rebonds », tels que la Russie, n'appliquant pas forcément les sanctions prises contre les pays d'utilisation finale.

La participation d'un intermédiaire à l'honorabilité « incertaine » dans un contrat fait peser des risques pour la société française : implication dans des rétro-commissions, voire de la corruption, perte ou rupture de contrat, atteinte réputationnelle, déstabilisation de la gouvernance, etc.

Les risques de détournement de biens à double usage ou de dissémination de matériels de guerre peuvent être réduits en conduisant des actions de vérification approfondie de l'honorabilité des clients et des intermédiaires. Ces actions sont de la responsabilité de la société contractante.

CAS CONCRET : SOLLICITATION D'UNE ENTREPRISE PRODUCTRICE DE BIENS À DOUBLE USAGE

Une société française commercialise des produits dans le domaine de l'optronique qui, en fonction de leurs caractéristiques techniques, sont classés parmi les biens à double usage ou matériels de guerre. Cette société est approchée par une entreprise étrangère, inconnue de ses juristes, pour lui fournir des matériels aux applications duales. Cette dernière déclare vouloir utiliser ces produits à des fins civiles dans son pays d'origine.

Sensibilisée par le Service, la société française informe la DRSD de ce nouveau prospect. Après vérification, le Service déconseille à la société de procéder aux exportations car le nouveau client s'avère être lié à un pays sous embargo et les produits seraient destinés à un emploi dans un conflit armé. La société française décide donc de ne pas donner suite à la sollicitation.

Si la relation commerciale avait eu lieu, elle aurait pu présenter un risque pour la réputation de la société et, par rebond, pour toutes ses activités. En effet, en cas d'identification de ses matériels dans un conflit armé, la société aurait pu être accusée de participer à un conflit en cours et aurait été passible de poursuites judiciaires avec de lourdes conséquences économiques.

Menace juridique : risque accru d'atteintes au contrôle des exportations

Principales recommandations

- ☐ Consulter les listes des entités sanctionnées par les États-Unis (https://sanctionssearch.ofac.treas.gov) et l'Union européenne (https://sanctionsmap.eu).

  Mises à jour régulièrement, ces listes ciblent les organismes (sociétés, universités) et les personnes physiques ayant été identifiés comme contributeurs à des programmes de développement d'armes de destructions massives (ADM) : nucléaire, biologique, chimique, vecteurs, technologiques de rupture. Cette contribution est mise en oeuvre par des exportations, du courtage, de l'assistance technique, du transit et des transferts de biens à double usage. Ces derniers comprennent des produits, y compris logiciels, technologies, savoir-faire immatériel (intangible) susceptibles d'avoir une utilisation tant civile que militaire.

- ☐ Contrôler l'existence réelle de l'entité : demande de documents officiels à l'entreprise (registre du commerce, ORBIS[9], etc.) ;
- ☐ Effectuer une veille en source ouverte sur l'entité pouvant mettre en avant des liens avec des sociétés ou pays défavorablement connus et/ou faire l'objet d'articles de presse défavorables ;
- ☐ Mettre en place un processus de contrôle aux exportations comportant une vérification de l'honorabilité des utilisateurs finaux et des éventuels intermédiaires, et se conformer à toutes les étapes du contrôle export, de l'amont (AFCI[10], licences, etc.) à l'aval (CNR[11], compte-rendu, etc.) ;
- ☐ Contacter la DRSD en cas d'incertitude sur l'honorabilité d'un intermédiaire ou d'un client potentiel.

CONTACTS :

- DGA : Mini-guide sur les exportations – www.armement.defense.gouv.fr
- Bien à double usage : doubleusage@finance.gouv.fr

Vous avez une question sur un projet d'exportation de biens à double usage : question.sbdu@finances.gouv.fr

[9] ORBIS : Base de données d'entreprises.
[10] AFCI : Autorisation de fabrication de commerce et d'intermédiation d'armement.
[11] CNR : Certificat de non-réexportation.

Menace réputationnelle : des atteintes insidieuses et croissantes

En 2023, les attaques provenant de mouvances contestataires, notamment antimilitaristes et anarchistes, se sont intensifiées. Ainsi, les modes opératoires font apparaitre des **organisations et des capacités de ciblage toujours plus structurées**.

La cause palestinienne a notamment été instrumentalisée par certaines mouvances contestataires et a donné lieu à plusieurs **manifestations pro-palestiniennes**, aux abords d'entreprises de défense ou de salons d'armement. D'autres actions visant les acteurs de la défense ont également pu être identifiées.

Ainsi, **un collectif associatif d'avocats a menacé de déposer plainte à l'encontre des salariés des sociétés exportatrices** qu'il accuse de participer directement ou indirectement à des crimes de guerre commis contre des civils palestiniens.

Ce phénomène pourrait s'intensifier selon l'évolution des conflits russo-ukrainien et israélo-palestinien ou encore à l'occasion des Jeux olympiques et paralympiques de Paris 2024, pour lesquels certaines entreprises de défense ont été sollicitées afin de contribuer aux dispositifs de sécurité.

CAS CONCRET : ATTEINTES RÉPUTATIONNELLES À L'ENCONTRE D'UNE SOCIÉTÉ EXPORTATRICE DE MATÉRIEL DE GUERRE

Présenté dans la presse comme ayant exporté du matériel de guerre potentiellement employé contre des civils en Ukraine et au Proche-Orient, un industriel de la défense est la cible de mouvances contestataires à l'initiative de différentes actions : blocage d'une usine, projection de peinture sur la façade du siège social, messages de dénigrement sur les réseaux sociaux, articles à charge dans la presse, pancartes incriminantes lors de manifestations.

L'accumulation de ces événements utilisée dans le cadre d'une campagne de dénigrement vient façonner un argumentaire et représente un risque important d'atteinte réputationnelle. Cela contribue au renforcement d'un narratif anti-militariste, qui présente les entreprises de la BITD comme responsables de crimes à l'encontre de populations civiles.

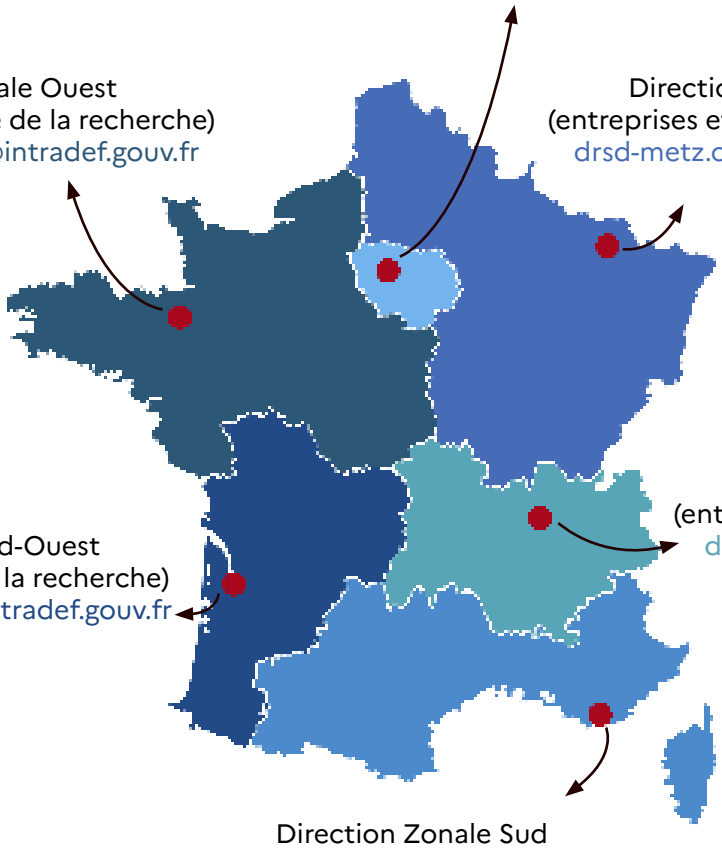
Gardons le contact

Direction Centrale
Section « Sensibilisation »
drsd-cie-sensibilisation.contact.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