LIE n°13 de la DRSD

Panorama des ingérences contre la sphère de défense

La lettre d'information économique
Juin 2023

Sommaire

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

Mesdames, Messieurs,

L'année 2022 aura été marquée par le retour d'une confrontation armée entre puissances en Europe. Ayant à l'esprit « l'hypothèse d'un engagement majeur » des armées françaises, le Président de la République a décidé d'adopter un modèle d'économie de guerre, devant aboutir à une plus grande résilience des capacités de production nationales.
Gage de puissance, la France se doit de disposer d'un système industriel complet, permettant de répondre, de façon pérenne, à une demande capacitaire requérant innovation et performance. Outre l'augmentation nécessaire de la production et la sécurisation de ses chaînes d'approvisionnement, ce changement de paradigme doit également promouvoir une vigilance renforcée face aux menaces d'espionnage, de sabotage et autres manœuvres de déstabilisation de compétiteurs étatiques comme infra-étatiques visant la base industrielle et technologique de défense (BITD).

La protection de cette dernière face à ces ingérences incombe directement à la Direction du Renseignement et de la Sécurité de la Défense (DRSD). Cette mission s'est traduite par un renforcement constant de nos échanges au contact de nos partenaires industriels (maîtres d'œuvre, sous-traitants, fournisseurs, start-ups, pôles de compétitivité, clusters), institutionnels et scientifiques détenteurs du potentiel scientifique et technique de la nation (PSTN). Cette mission d'accompagnement s'est notamment manifestée par une augmentation du rythme d'actions de sensibilisation spécifiques à chaque entité.
Cette LIE a donc pour objectif de partager avec vous nos constats sur l'état des menaces pesant sur le tissu industriel de défense (les principaux modes opératoires, les principaux acteurs ingérants et les secteurs convoités), afin que vous puissiez adopter ou confirmer une posture de vigilance appropriée.

Dans cette optique, je souhaite attirer votre attention sur l'importance de maintenir notre dynamique d'échanges, notamment la remontée d'informations, entre la DRSD et l'ensemble des acteurs de la sphère de défense, collaborant ainsi à garantir notre souveraineté nationale et notre autonomie stratégique, plus que jamais indispensable.

Je vous assure que toutes nos équipes, présentes à vos côtés, restent mobilisées pour vous accompagner dans vos démarches de prévention, de sensibilisation et de protection afin de devancer toutes les atteintes.

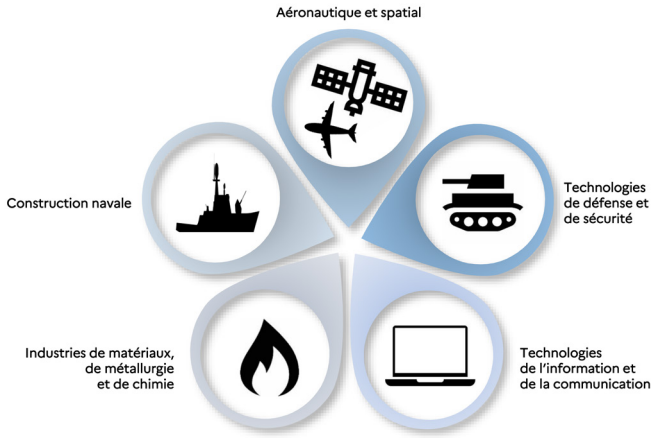
Général de corps d'armée Philippe Susnjara
Directeur du Renseignement et de la Sécurité de la Défense

Synthèse des ingérences constatées

En 2022, la DRSD a détecté un nombre élevé d'ingérences à l'encontre des emprises de la sphère de défense, mais constant par rapport aux années précédentes.

En dépit du conflit russo-ukrainien et des risques d'ingérences associés (cf. LIE spéciales : « Ukraine » (avril 2022) et « Économie de guerre » (sept. 2022)), les industriels de la BITD ont également pâti des effets économiques induits par ce conflit. Les tensions sur l'approvisionnement des matières premières et l'augmentation du coût de l'énergie se sont dès lors ajoutées aux impacts déjà constatés.

La plupart des secteurs ont suscité l'intérêt des compétiteurs stratégiques des industriels français, d'ores-et-déjà bien connus pour leur conduite offensive. Leurs objectifs sont variés : pallier des besoins opérationnels immédiats, des déficits sur des marchés hautement concurrentiels ou des stratégies d'investissement sur des technologies de ruptures, etc. Ceux-ci usent davantage de stratégies indirectes, passant par des actions de débauchage ciblées, l'exploitation de contraintes juridiques ou des pratiques de lobbying agressives, favorisant leurs propres normes.

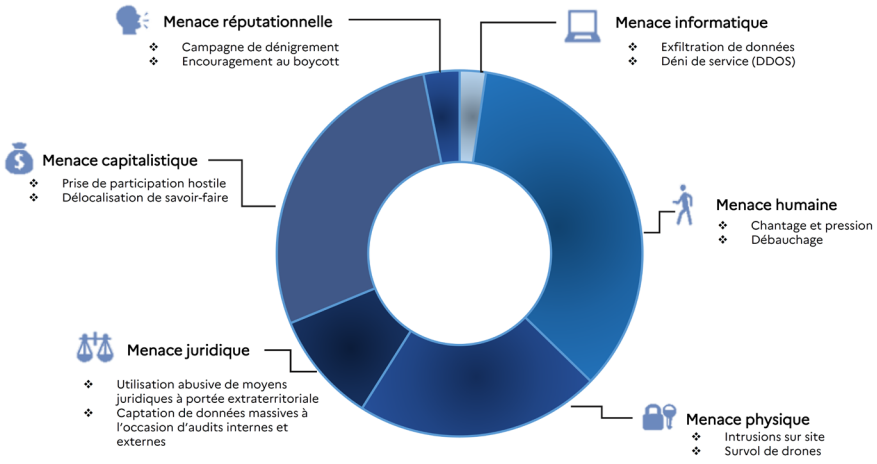


En outre, le contexte international marqué par un retour potentiel à une ère de conflits de haute intensité favorise des investissements étrangers plus conséquents dans le secteur de la défense. Ces investissements, s'ils sont nécessaires à l'activité industrielle, peuvent aussi présager de manœuvres de prédation capitalistique ciblant les savoir-faire français de pointe.

S'agissant de la menace cybernétique, cette dernière reste particulièrement active et se confirme au premier trimestre 2023. Elle a notamment été marquée par une forte activité cybercriminelle affectant **l'ensemble des secteurs d'activités** de la BITD.

Dans l'hypothèse d'une escalade du conflit, les modes opératoires envers la BITD pourraient se diversifier et se multiplier.

Infractions les plus fréquentes



MENACE HUMAINE : UNE RECRUDESCENCE DE CAS CONSTATÉS

Le nombre d'atteintes dites « *humaines* » (chantage, faux entretiens de recrutement, vols d'ordinateur, tentatives de débauchage) n'a cessé de croître depuis la crise du COVID.
En effet, certains collaborateurs possédant un savoir-faire spécifique et un accès fonctionnel et / ou numérique à des informations sensibles semblent constituer un vivier davantage ciblé.

Vols d'ordinateurs

L'un des traits majeurs de l'année 2022 est la hausse des vols d'opportunité. Les informations dérobées revêtent la plupart du temps un caractère sensible et stratégique pour l'entreprise (activités techniques, financières, comptables…) dont la perte peut occasionner un préjudice majeur (captation de savoir-faire, liste de clients et fournisseurs). Ce ciblage concerne tant les outils de travail professionnels que personnels, dès lors qu'ils sont utilisés dans le cadre de réunions, déplacements professionnels.

CAS CONCRETS

- En 2022, à l'occasion d'un déplacement en Asie du Sud-Est, le manager d'une entreprise de la BITD spécialisée dans le quantique, s'est absenté quelques minutes de sa chambre d'hôtel pour régler une formalité administrative avec le personnel. Ce court laps de temps a pourtant suffi à un individu pour lui dérober son ordinateur professionnel laissé dans sa chambre. En possession d'un badge électromagnétique d'entrée, il estimait que sa chambre était suffisamment sécurisée.

- Récemment recruté par un sous-traitant de rang 3 spécialisé dans l'optique, un apprenti patiente plusieurs semaines avant de recevoir son matériel de travail. Afin de pouvoir remplir ses missions au cours de cette période, il utilise son ordinateur personnel avec l'approbation de ses supérieurs. Pendant ses congés, il se fait dérober son ordinateur et son téléphone personnels sur une aire d'autoroute. Ce dernier contenait de nombreuses données personnelles mais également toutes les données relatives à son activité au profit de l'entreprise. A posteriori, la remontée d'informations auprès de son officier de sécurité et de la DRSD a permis de sensibiliser ses collègues à ce risque.

RECOMMANDATIONS

Les périodes estivales approchant, voici quelques recommandations afin de limiter le vol d'ordinateurs et de supports numériques :

- **N'emporter avec soi que les données et supports numériques strictement nécessaires ;**
- Ne jamais laisser ordinateurs ou téléphones sans surveillance (voitures personnelle ou de location, transports, hôtels, salle de sport, restauration) ;
- Séparer vie professionnelle et vie personnelle par l'utilisation de supports électroniques distincts.

Débauchage

Les compétences-clé de certains collaborateurs experts peuvent faire l'objet de convoitises. Pour se les accaparer, des stratégies de recrutement offensives et planifiées dans la durée sont mises en place par des compétiteurs étatiques et des concurrents étrangers. Les partenariats mis en place par ces derniers peuvent en effet faciliter l'identification d'éléments prometteurs au sein d'écoles, de centres de recherche ou d'entreprises françaises, ou encore cibler directement des transferts de technologies insuffisamment encadrés.

RECOMMANDATION

- Les clauses de confidentialité et de non-concurrence sont des mesures préventives primordiales pour contribuer à la protection de cette ressource humaine.

CAS CONCRET

Un chercheur français spécialisé dans le domaine des lasers s'est vu offrir, après plusieurs rendez-vous initiés par les diplomates d'une ambassade, un poste d'intervenant dans une université prestigieuse du Moyen-Orient. Malgré la proposition de prise en charge de tous ses frais et d'une rémunération importante, le chercheur, sensibilisé aux risques de captation des travaux de recherche, a refusé l'offre de poste après avoir compris que l'intégralité de ses recherches seraient sous le contrôle exclusif du pays d'accueil. Régulièrement en contact avec son agent référent de la DRSD, le chercheur n'a pas hésité à lui faire part de ses sollicitations.

ATTEINTE RÉPUTATIONNELLE : MENACE INSIDIEUSE ET CROISSANTE

Conscients de l'importance de la réputation positive légitimement acquise par les entreprises françaises - en particulier de défense – des acteurs malintentionnés y attentent de manière sophistiquée et continue, quoi qu'il en soit toujours déstabilisatrice. Prenant pour cible la performance d'un produit ou la conduite commerciale elle-même de l'entreprise, voire sa conformité à des normes d'hygiène ou environnementales, les prétextes sont multiples et mettent à mal la compétitivité des industries françaises. Relayées par voie de presse, numérique ou simplement par le bouche à oreille, ces atteintes engendrent des conséquences multiples et protéiformes. En effet, qu'il s'agisse de la diffusion d'informations confidentielles sur la conception d'un produit et la copie du savoir-faire attenant, de la perte de confiance de clients ou fournisseurs suite à la publication d'un rançonnage, les atteintes réputationnelles peuvent durablement mettre à mal toutes les entreprises de défense françaises, de la start-up au grand groupe, en passant par le tissu de TPE, PME et ETI.

CAS CONCRET

Il y a quelques années, un grand groupe industriel a vu le cours de son action chuter de près de 20% à la suite d'une attaque informationnelle. Une rumeur concernant de potentielles malversations financières orchestrées par le groupe avait circulé par la publication de faux communiqués officiels sur un faux site web créé pour l'occasion. En dépit des preuves apportées par l'entreprise sur le montage de cette campagne de désinformation, l'objectif de déstabilisation même momentanée était atteint.

RECOMMANDATIONS

- Prévenir : établir une charte de « bon usage » des réseaux sociaux à l'attention des collaborateurs sensibilisés aux risques d'utilisation ;
- Détecter : effectuer (si possible) une veille relative à votre écosystème et sur vos propres réseaux ;
- Gérer : prendre en compte la gestion d'analyse de risques (dont RETEX) et définir une communication de crise.

MENACE JURIDIQUE : UN USAGE DÉCOMPLEXÉ DU DROIT À DES FINS STRATÉGIQUES (*"lawfare"*)

La menace des ingérences fondées sur un usage stratégique des lois à portée extraterritoriale et de la norme par nos compétiteurs s'intensifie dans plusieurs directions.
Les États-Unis, exploitant la portée extraterritoriale de leur droit national, continuent d'entretenir une application très contraignante de leurs dispositifs législatifs et normatifs. En s'appuyant sur la vérification de la conformité à certaines règlementations (ITAR et EAR), l'administration américaine peut ainsi visiter des entités de la BITD, y compris sur le territoire national.
En parallèle, la Chine poursuit l'élaboration d'une stratégie similaire par l'adoption de lois à portée potentiellement extraterritoriale, notamment en matière de contrôle des exportations et de régulation du numérique. S'agissant du contrôle des exportations, l'assiette d'application des nouvelles règlementations est particulièrement large, puisque l'interdiction d'exporter des biens s'applique à tous ceux « *liés à la préservation de la sécurité nationale et des intérêts nationaux chinois* », y compris lorsqu'il s'agit uniquement de prestations intellectuelles.
Ainsi, la conformité à l'ensemble de ces normes peut avoir un impact direct sur l'activité économique des entreprises de défense françaises (transferts non maîtrisés de données, processus internes de mise en conformité, audits externes, voire poursuites pouvant induire des sanctions pénales et financières).

CAS CONCRET

Dans le cadre d'une réglementation étrangère à laquelle elle doit se conformer, une entreprise française liée à la sphère de défense accepte d'être l'objet d'un contrôle mené par un membre de l'administration de cet Etat. L'audit ne révèle aucun cas de non-conformité et l'entreprise expose sa maîtrise de la réglementation en question. Cependant, tout au long du contrôle, l'auditeur pose des questions qui s'éloignent finalement du cadre prévu par l'audit, mais qui répondent aux centres d'intérêt in fine concurrentiels d'un tiers.

Les entreprises de la sphère de défense sollicitées par une administration étrangère dans le cadre d'un audit de conformité peuvent demander à être accompagnées par l'État.

Points de contact : SGDSN, DISSE, DRSD.

RECOMMANDATIONS

- Mettre en place ou s'abonner (si possible) à une **veille juridique** incluant les pays au sein desquels l'entreprise développe son activité ;
- En cas d'inspections ou d'**audits externes** d'un cabinet ou d'une autorité : préparer cette démarche en collaboration avec vos interlocuteurs de la DRSD (informer vos collaborateurs, s'en tenir au cadre strict de l'audit, écarter les sujets potentiellement sensibles, faire suivre un parcours de notoriété) ;
- En cas de **demande de documents** d'une autorité étrangère dans le cadre d'une procédure administrative ou judiciaire : **saisir le SISSE** (*via* les DISSE) afin de préciser les implications de cette demande au regard de **la loi 68-678 du 26 juillet 1968 dite « d'aiguillage » ou « de blocage ».**

Ingérences physiques visant les emprises

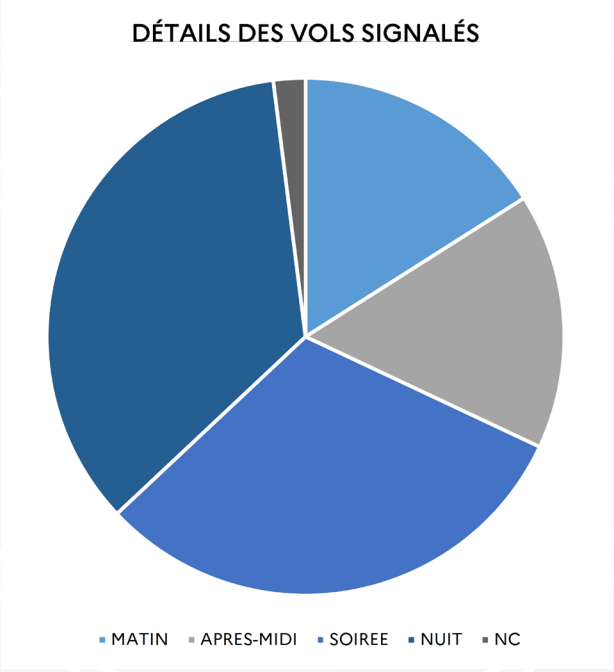
MENACE PHYSIQUE : INTRUSION PAR SURVOL DE DRONES

En 2022, la DRSD a constaté une tendance à la hausse des survols de drones au-dessus des emprises de la sphère de défense. Celles-ci sont vulnérables, car peu habituées à réagir à ce type d'intrusion.

En raison de la facilité d'acquisition du drone de loisirs ou professionnel, ainsi que de moyens réduits - tant juridiques que techniques - dans le domaine de la lutte anti-drones, la menace est croissante.

Pour leur part, les survols nocturnes sont en forte augmentation depuis 2022, traduisant vraisemblablement un ciblage des emprises ainsi que l'utilisation d'optronique spécialisée.

La **remontée d'informations vers vos agents DRSD est donc primordiale** pour vous accompagner dans la mise en place de processus internes facilitant la réaction face à ce nouveau mode d'ingérence.



POINTS DE VIGILANCE

- Si vous constatez un vol de drone en simultané et/ ou en formation :
- Si vous constatez la répétition de survols sur certains sites ou sur une même entité :

» Appliquer les recommandations suivantes :

- systématiser (autant que possible) les remontées d'incident et de suivi auprès de votre chaîne hiérarchique et / ou de votre interlocuteur local de la DRSD ;
- mettre en place des fiches réflexes ainsi que des exercices de simulation ;
- renforcer la vigilance de vos collaborateurs ainsi que vos prestataires au travers de sensibilisations, et les former à la rédaction de rapport d'étonnement.

Ingérences cybernétiques

Depuis le second semestre 2022, le Service a observé une résurgence d'attaques par déni de service distribué (DDOS).

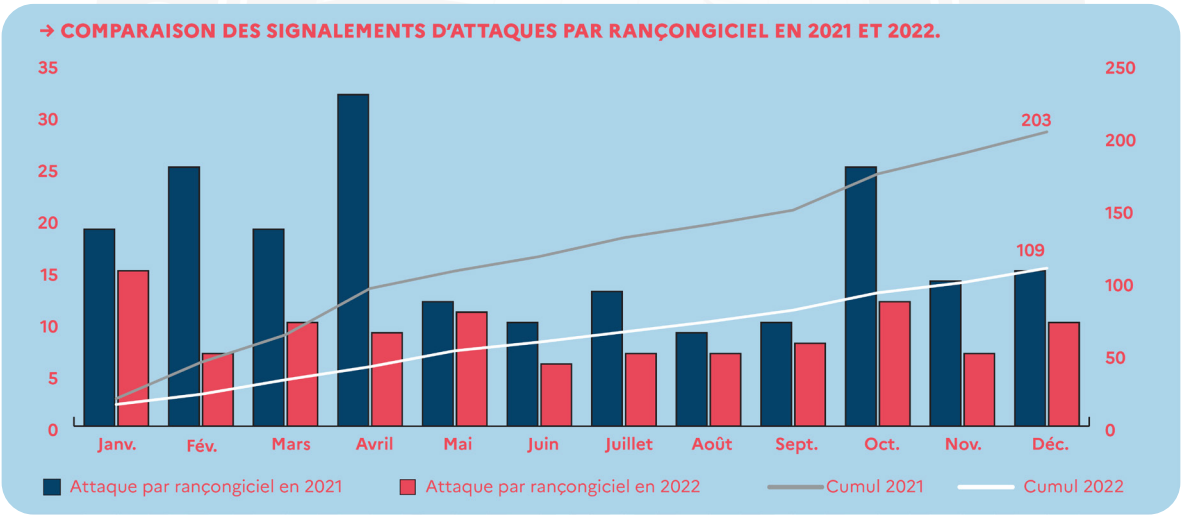
Une résurgence notable des attaques par DDOS

Une résurgence sensible des attaques par DDOS depuis l'automne 2022 est constatée. Des organismes politiques tels que le Parlement européen ont été ciblés, notamment à la suite de prises de position en soutien à l'Ukraine.
Généralement ce type d'attaque n'entraîne ni destruction ni vol de données mais une indisponibilité des services, notamment vis-à-vis du public. La technicité mise en œuvre est plus faible que celle qui est déployée pour mener l'infiltration d'un système à des fins d'espionnage ou de sabotage. Elle est donc à la portée d'un plus grand nombre d'opérateurs, souvent amateurs.

*Une attaque par « **déni de service distribué** » vise à saturer de manière coordonnée un système exposé sur Internet.*

Une diminution des rançongiciels précédant leur remontée en puissance ?

L'année 2022 a vu de nombreuses attaques par rançongiciels cibler des entreprises de la BITD. La publication des données exfiltrées lors de ces attaques peut parfois survenir jusqu'à une dizaine de mois après l'attaque. Certaines attaques survenues en 2022 pourraient ainsi continuer à manifester leurs effets en 2023.
Bien qu'une diminution des attaques par rançongiciels visant la France – et comprenant ses entreprises de défense - soit à noter, celle-ci ne doit pas entraîner pour autant une diminution des mesures cyberdéfensives. En effet, la reprise d'activités des rançongiciels semble amorcée depuis la fin de l'année 2022.



Source CERT FR : https://www.cert.ssi.gouv.fr/uploads/CERTFR-2023-CTI-001.pdf

*Les attaques par **rançongiciel** sont d'exécution dite « rapide ». Leur objectif reste majoritairement pécuniaire.*

Marquée par le conflit russo-ukrainien, l'année 2022 a été celle de la diversification des cybermenaces. La résurgence de modes opératoires subversifs (effacements de sites, DDOS) dont l'impact direct sur l'activité des entreprises est faible, s'est accompagnée d'une persistance de la menace par rançongiciel, qui demeure majeure. Les actions de cyber-espionnage, peu nombreuses mais toujours d'un niveau de technicité élevé, doivent demeurer un point d'attention des équipes de cyberdéfense.

La BITD doit donc maintenir sa vigilance, en considérant que **tout industriel dont le nom est associé à un soutien à l'effort de guerre ukrainien peut être victime de cyber attaque par représailles**, pouvant prendre les formes susmentionnées.

Lancement du Computer Emergency Response Team de la DRSD

À compter du 21 juin 2023, la DRSD déploie le *CERT [ED]*, centre de réaction cyber au profit des Entreprises de la Défense.

Réponse à incident

Le *CERT [ED]* **traite tous les types** d'incidents de cybersécurité qui surviennent ou menacent de survenir au sein du périmètre de la sphère de défense.

Le *CERT [ED]* accompagne les administrateurs et exploitants de systèmes dans la gestion des aspects techniques et organisationnels des incidents. En particulier, il fournit une assistance ou des conseils pour la catégorisation des incidents et leur coordination. Il s'agit avant tout de répondre présent au côté des victimes et de leur apporter un soutien circonstancié dans le traitement de l'incident.

Veille en vulnérabilités

Le *CERT [ED]* agit à titre préventif, en recensant et en identifiant les vulnérabilités publiques de sécurité numérique susceptibles d'être exploitées sur des systèmes d'information de la sphère de défense.

Le *CERT [ED]* est en mesure de veiller les annonces sur les vulnérabilités concernant des logiciels ou matériels spécifiques et d'alerter les parties concernées.

Sensibilisation, accompagnement

Le *CERT [ED]* participe aux actions de sensibilisation au profit de la sphère de défense.

Le *CERT [ED]* partage ses connaissances et son expérience en sensibilisant les entreprises de défense sur les sujets de cyber sécurité.

Dans le cadre de ses missions, le *CERT [ED]* coopère avec l'écosystème cyber national et poursuit le développement de synergies avec ses partenaires.

Nous contacter :

- Boîte fonctionnelle : cert-drsd.contact.fct@def.gouv.fr
- Numéro vert : **0 805 046 300**

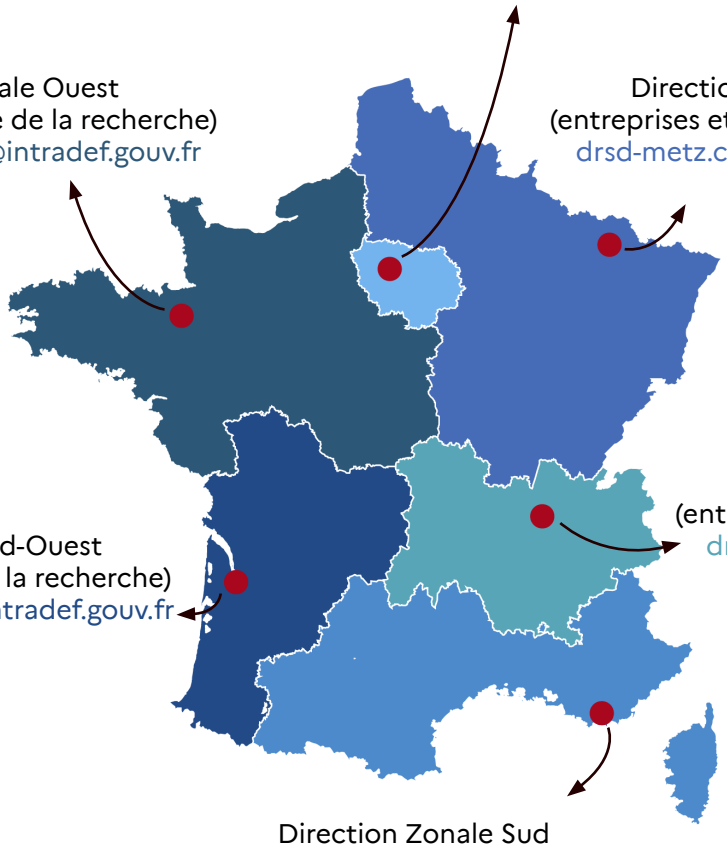
Gardons le contact

Direction Centrale
Section « Sensibilisation »
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

Directions Zonales 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

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