LIE n°17 de la DRSD

Le référentiel de maturité cyber (RMC) des entités de la sphère défense

La lettre d'information économique
Décembre 2024

Sommaire

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

Mesdames, Messieurs,

Notre *Lettre d'information économique n°16 « Panorama des ingérences à l'encontre de la sphère défense en 2023 »* a rappelé que les attaques à but lucratif issues de l'écosystème cybercriminel sont restées l'une des principales menaces pour la base industrielle et technologique de défense (BITD) l'an passé. La montée en maturité cyber constitue donc un impératif pour la pérennité des entreprises et la continuité de leur activités, face à des menaces toujours croissantes et de plus en plus sophistiquées.

Si les cyberattaques constituent une menace pour l'ensemble du tissu industriel français, la BITD représente une cible à haute valeur ajoutée en raison de sa contribution aux capacités de défense françaises, a fortiori dans un contexte géopolitique qui se durcit depuis plusieurs années. Dans ce cadre, les PME et ETI sont particulièrement vulnérables et peuvent servir de rebond pour atteindre, par latéralisation, des systèmes d'information d'autres entreprises (maitres d'œuvre, autres sous-traitants, etc.).

Au-delà du simple appât du gain, les objectifs de ces cyberattaques peuvent être multiples : espionnage en captant les données à des fins de rattrapage technologique, sabotage en bloquant le développement d'un programme ou d'une ligne de production, atteinte à l'image de marque ou à la réputation de sociétés face à leurs principaux concurrents. La DRSD souhaite à travers cette LIE vous sensibiliser à nouveau à cette menace et vous informer de l'existence du référentiel de maturité cyber (RMC), conçu pour améliorer la protection des systèmes d'informations de vos structures.
Cette LIE vise également à vous présenter le Diagnostic cyber défense de la Direction générale de l'armement (DGA), dispositif d'aide mis en œuvre conjointement avec Bpifrance pour vous aider à financer l'analyse de risques de vos réseaux et votre montée en maturité cyber.

Enfin, soyez assurés que nos agents se tiennent à vos côtés pour vous conseiller et vous accompagner dans l'adaptation de votre niveau de protection pour faire face à l'ensemble du spectre des menaces numériques et ainsi préserver votre patrimoine matériel et immatériel, nécessaire à la consolidation de notre souveraineté nationale.

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

La présentation du référentiel de maturité cyber (RMC) de la DGA

Le RMC a pour objectif de simplifier et d'harmoniser les exigences cybernétiques des donneurs d'ordres étatiques et industriels. Il s'inscrit dans une démarche progressive d'amélioration du niveau de cybersécurité des réseaux informatiques d'usage courant des entreprises de la BITD.

Ce référentiel peut être utilisé :
- **de manière contractuelle**, par un donneur d'ordre vers un de ses sous-traitants ou un fournisseur pour évaluer son niveau de maturité cyber ;
- **dans le cadre d'un processus d'auto-évaluation** par une entreprise pour valoriser son niveau de maturité cyber auprès de ses donneurs d'ordre.

LE RMC SE COMPOSE DE TROIS NIVEAUX AUX EXIGENCES PROGRESSIVES

Le premier niveau, intitulé « *fondamental* », comprend 21 exigences élémentaires. Il va s'imposer contractuellement dans les relations entre la DGA et l'industrie de défense.

Le niveau « *fondamental* » a été conçu pour proposer des mesures organisationnelles simples et des mesures techniques fondées sur une configuration adaptée des systèmes d'exploitation ou de logiciels très standards comme les anti-virus. La mise en conformité ne nécessite pas d'investissement important ou de logiciel spécialisé.
Ce niveau vise à assurer une sécurité minimale des systèmes d'information (SI) utilisés pour la réalisation des contrats identifiés par le donneur d'ordre comme concourant à des activités de défense. Les contrats traitant d'informations **protégées** (DR - Diffusion restreinte) et **classifiées** (S - Secret ou TS - Très Secret) sont déjà soumis à des textes règlementaires spécifiques (IGI 1300, IM 900 et II 901), précisés dans les plans contractuels de sécurité (PCS) ou les clauses des contrats et ne sont donc pas concernés par le RMC.

Par conséquent, le niveau « *fondamental* » constitue une première étape de certification de maturité cyber. Il sera complété par des niveaux supérieurs qui s'appuient sur les règles issues de la transposition de la directive européenne *NIS 2*[1] en droit français pour assurer l'équivalence avec le maximum de référentiels existants. Au regard des critères exposés dans cette directive, seront définies des « *entités importantes* » et des « *entités essentielles* ». À ces définitions correspondront un **premier niveau**, en phase avec les exigences *NIS 2* demandées aux « *entités importantes* », et un **deuxième niveau**, en phase avec celles demandées aux « *entités essentielles* ».

CES 21 EXIGENCES :

- concernent de nombreux domaines répertoriés, de la **gouvernance** à la **gestion des incidents** ;
- sont applicables avec un **effort mesuré** par les plus petites structures ;
- visent les systèmes d'information utilisés pour la réalisation de contrats identifiés comme **concourant à des activités de défense**.

[1] Directive « *Network and Information Security 2* » (NIS 2) : **Journal officiel de l'Union européenne L 333/80 du 27 décembre 2022**.

La présentation du référentiel de maturité cyber (RMC) de la DGA

QUESTIONS FRÉQUENTES :

Le RMC est-il une obligation ?

Le niveau « *fondamental* » sera progressivement exigible au titre des clauses contractuelles.

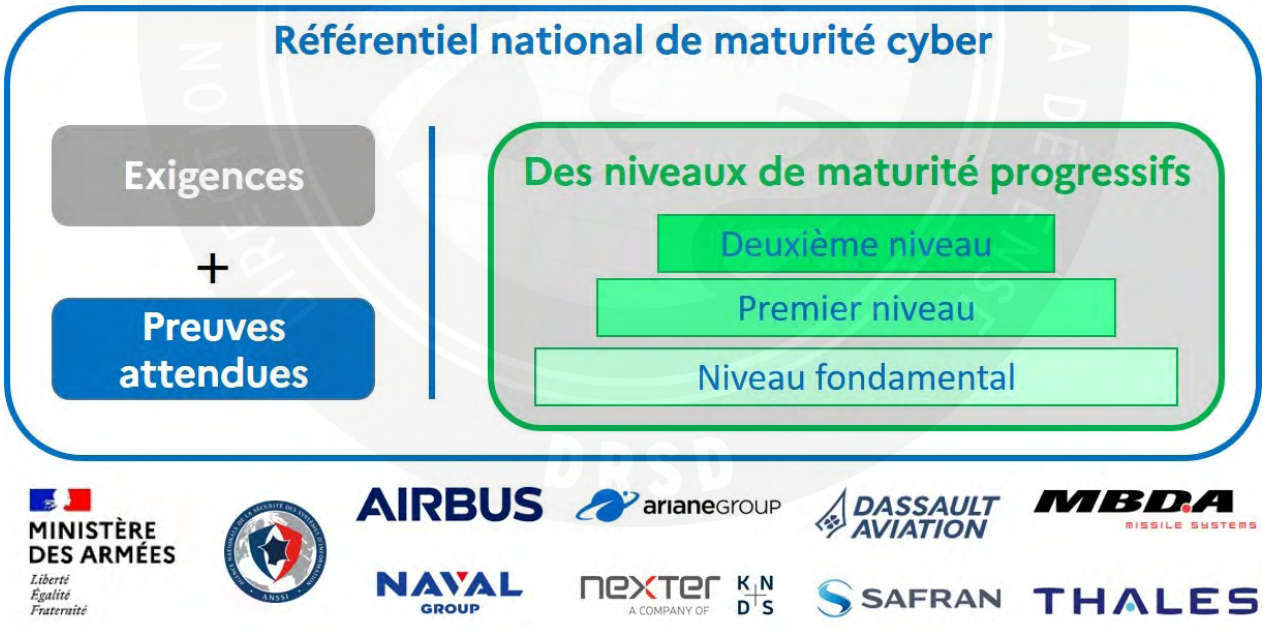
Concrètement : l'entreprise devra avoir réalisé une auto-évaluation du niveau de maturité cyber de son SI par rapport aux règles du RMC (sous forme déclarative pouvant déboucher sur une revue des preuves en cas de besoin).

Comment faire la déclaration ?

Les entreprises pourront remplir le questionnaire accessible sur le portail de l'armement (www.armement.defense.gouv.fr). Le niveau « *fondamental* » est considéré comme « atteint » lorsque les réponses aux exigences se situent toutes dans la colonne J et au-delà.

Quelle est la durée de validité ?

L'attestation délivrée par la DGA pour les futurs niveaux n'excèdera pas trois ans.



La présentation du référentiel de maturité cyber (RMC) de la DGA

AUTRES OBJECTIFS DU RMC :

- **éviter l'exclusion** des marchés internationaux ;
- **réduire les risques d'ingérences économiques** en cas d'audits par un tiers étranger ;
- **limiter la multiplication des normes** pesant sur les entreprises de la défense. Pour ce faire, des négociations sont en cours pour obtenir une équivalence avec certains référentiels internationaux tels que la *Cyber Maturity Model Certification* (CMMC) niveau 1 (niveau de sécurité minimale).

Référentiel de maturité cyber

armement.defense.gouv.fr/securite-et-habilitation/securite-du-numerique/referentiel-de-maturite-cyber

Documents mis à disposition :
- une description du contexte et de la manière d'utiliser le référentiel ;
- un tableau des exigences commentées et des preuves à produire.

Contacts utiles :
- DGA (Délégation générale de l'armement) : dga-ssdi-dossi.conseiller-industriel.fct@intradef.gouv.fr
- CERT [ED] (Centre de réponse à incident [*Computer Emergency Response Team*] au profit du secteur des entreprises de défense) : cert-drsd.contact@def.gouv.fr

Pour aller plus loin, l'ANSSI met à disposition en libre accès les guides suivants :
- *Maîtrise du risque numérique. L'atout de confiance.*
- *La cybersécurité pour les TPE/PME en 12 questions.*
- *Organiser un exercice de gestion de crise cyber.*

[2] La *Cybersecurity Maturity Model Certification* (CMMC) (1) est une norme développée par le *Department of Defense* (DoD) américain depuis 2018 et publiée le 26 décembre 2023. La conformité à la CMMC sera intégrée dans les appels d'offres à venir du DoD et sera imposée à tous ses sous-traitants, y compris étrangers. Or, dans certains cas, la norme imposera la réalisation d'audits externes par des entités américaines accréditées. Depuis 2020, en coordination avec l'ANSSI et la DGA, la DRSD accompagne les entreprises concernées par la CMMC.

Voir LIE n°14 de novembre 2023 – « Le lawfare ou l'usage du droit à des fins stratégiques ».

Le dispositif d'aide à la cyber sécurisation de la DGA : le « DIAGCYBER »

Financé par la DGA dans le cadre de son plan d'action en faveur des ETI, PME et start-ups « PEPS », et mis en œuvre conjointement avec Bpifrance, le diagnostic cybersécurité vise à subventionner les PME et ETI volontaires pour réaliser une analyse de risques de leurs réseaux et prendre en charge, en partie, leurs frais de sécurisation.

Objectif principal : pérenniser la sécurité des systèmes d'information non protégés des entreprises en lien avec le ministère des Armées.

RÉALISÉ PAR DES PRESTATAIRES D'AUDITS DE SÉCURITÉ DES SI (PASSI), LE DIAGCYBER SE DÉROULE EN TROIS PHASES :

- **Phase 1** : réalisation par des PASSI d'un audit de sécurité des SI pour identifier les risques numériques liés à l'entreprise et évaluer la sécurité des SI ;
- **Phase 2** : accompagnement de la mise en œuvre des recommandations de la première phase et acquisition de solutions de cyber-sécurisation ;
- **Phase 3** : nouvel audit de vérification à l'issue de cette mise en œuvre.

BÉNÉFICIAIRES ÉLIGIBLES	DÉPENSES ÉLIGIBLES
Toutes PME - ETI de la sphère défense de moins de 2 000 salariés	50 % du montant de l'expertise - forfait maximum : 8 800 € HT

Les trois volets de l'intervention des agents de la DRSD dans le cadre cyber

En premier lieu, la DRSD accompagne la montée en maturité cyber des entreprises sous contrat défense par la réalisation d'inspections et de contrôles des systèmes d'informations directement liés à des activités de défense.

→ **Ces inspections et contrôles servent à vérifier que les niveaux d'exigence cyber précisés dans les contrats de marchés défense sont bien atteints par les entreprises.**

En outre, le Service appuie les entreprises par la réalisation de sensibilisations au profit des COMEX, CODIR, collaborateurs, sous-traitants etc, des entités de la BITD.

Enfin, la DRSD conseille les entreprises dans leur mise en conformité vis-à-vis de la règlementation à laquelle elles sont soumises dans le cadre de marchés de défense (ex. : non-conformité à une exigence règlementaire impossible à corriger au préalable).

CAS CONCRET : TENTATIVE DE VOL DE DONNÉES DE RECHERCHE *VIA* UNE MESSAGERIE

Faits :

Un organisme de recherche français, spécialisé dans le nucléaire, a été victime de plusieurs tentatives de vol de données concernant des prototypes de logiciels qu'il conçoit. Le ou les auteurs ont usurpé l'adresse mail d'un des cadres pour récupérer les informations sensibles relatives aux travaux de recherche et développement. Après plusieurs tentatives infructueuses, une plainte a été déposée mais l'enquête n'a pas permis d'identifier les auteurs, localisés à l'étranger.

Conséquences :

Ces actions ont vraisemblablement été commanditées par un concurrent étranger qui cherchait à bénéficier des avancées de cette entité de recherche française.
En cas de réussite, le vol de données aurait fait peser un sérieux risque sur la pérennité de l'organisme de recherche. Une démarche interne doit être entreprise pour mieux percevoir les risques et les vulnérabilités qui pèsent sur toute l'activité de recherche et de développement des logiciels et renforcer sa protection pour déjouer toute nouvelle tentative du même type.

Les trois volets de l'intervention des agents de la DRSD dans le cadre cyber

Recommandations

L'organisme a été victime de plusieurs tentatives :

- ☐ sensibiliser régulièrement le personnel sur ce type de risque avec la consigne de signaler immédiatement toute approche inhabituelle ;
- ☐ sensibiliser systématiquement chaque nouvel arrivant à la protection des informations ;
- ☐ signaler les faits dès la première tentative et le plus rapidement possible.

L'adresse mail d'un cadre a été usurpée :

- ☐ prendre du recul par rapport à l'urgence de répondre à une sollicitation inhabituelle ou surprenante ;
- ☐ au moindre doute : ne pas cliquer (lien ou pièce-jointe) et ne pas transférer ;
- ☐ contacter l'expéditeur présumé par un autre canal pour confirmer sa demande ;
- ☐ renforcer la sécurité des systèmes d'information et particulièrement l'environnement des messageries ;
- ☐ mettre en place (ou compléter) une charte informatique pour un usage sécurisé des outils informatiques, notamment en ce qui concerne le partage et le stockage des informations sensibles.

Les travaux de R&D sont ciblés :

- ☐ vérifier - et au besoin renforcer - le niveau de protection des informations de R&D (protection physique, informatique et juridique) ;
- ☐ identifier et catégoriser les informations en fonction de leur sensibilité. Ce travail doit être effectué à chaque nouveau projet de R&D pour assurer une protection adaptée.

L'origine de l'attaque n'a pu être précisée :

- ☐ une analyse de la situation concurrentielle doit être effectuée pour mieux percevoir les risques existants et futurs dans le but de renforcer la protection des informations susceptibles d'être convoitées ;
- ☐ vérifier si d'autres faits inhabituels liés aux tentatives de vol se sont produits. Si c'est le cas, les intégrer à l'analyse mentionnée ci-dessus.

Il s'agit de travaux de recherche en lien avec la sphère défense :

- ☐ informer la DRSD de ces faits qui entrent dans le champ de ses missions de contre-ingérence économique.

La DRSD sera en mesure de conduire des actions de sensibilisation sur la protection des informations et la contre-ingérence économique auprès du personnel et de la direction de l'organisme de recherche.

Les trois volets de l'intervention des agents de la DRSD dans le cadre cyber

CAS CONCRET - VOL DE DONNÉES *VIA* UNE CYBERATTAQUE VISANT UN LOGICIEL RH

Faits :

Une cyberattaque est survenue chez un des prestataires RH d'une société de défense française. Cette attaque consistait en l'exploitation d'une faille *zero day* d'un logiciel RH utilisé par la société.

Un mois après l'attaque, un ingénieur de l'entreprise en charge du développement d'un prototype innovant pour les armées françaises, en télétravail, a subi un cambriolage alors qu'il s'était absenté de son domicile durant sa pause déjeuner. A son retour, il a constaté la disparition de son ordinateur et de son téléphone professionnels. En infraction avec la PSSI de son entreprise, son ordinateur et son téléphone contenaient des données sensibles (marches, fournisseurs, prix, etc.) stockées physiquement sur les appareils en question plutôt que sur des serveurs internes à l'entreprise accessibles par VPN.

Conséquences :

S'il est impossible d'écarter définitivement l'hypothèse d'un vol opportuniste, ce cambriolage présentait un faisceau d'indices permettant d'envisager une opération ciblée. En effet, les informations ayant permis ce cambriolage (identité, adresse, appartenance à la société, jours pointés en télétravail de l'intéressé, etc.) figuraient parmi les données exfiltrées lors de la cyberattaque. De plus, le salarié disposait d'une empreinte numérique bien maîtrisée (*LinkedIn*) qui ne faisait pas apparaitre ces informations. La probabilité que cette exfiltration de données de la cyberattaque du logiciel RH ait été exploitée à des fins de malveillance pour cibler ce collaborateur en particulier est renforcée.

Recommandations

- ☐ informer l'officier de sécurité qui transmettra l'information à la DRSD. Cette dernière sera en mesure de conduire des investigations et de vous accompagner dans les actions correctives ;
- ☐ porter plainte auprès des forces de sécurité intérieure (police ou gendarmerie) ;
- ☐ identifier les données volées et les conséquences pour l'entreprise ;
- ☐ prévoir (si possible) un accès sécurisé à distance pour les informations sensibles ;
- ☐ privilégier l'usage d'un VPN pour sécuriser les échanges des salariés de l'entreprise lors d'une connexion à un réseau tiers ;
- ☐ sensibiliser régulièrement vos collaborateurs, notamment sur les risques numériques ainsi qu'aux bons usages sur les réseaux sociaux (ex. : clause d'utilisation).

DGA et MBDA : regards croisés sur le développement de la maturité cyber au sein de la BITD

Le 27 octobre 2023, l'État et huit maîtres d'œuvre industriels (AIRBUS, ARIANE GROUP, DASSAULT, KNDS, MBDA, NAVAL GROUP, SAFRAN, THALES) ont présenté conjointement les intérêts d'une montée en maturité cyber de toute la BITD. Le socle commun (RMC) présenté en séance a pour vocation d'être intégré dans les exigences contractuelles puis dans la réglementation française avec la transposition de la NIS2 en droit français. L'ensemble de la démarche contribue à l'amélioration de la robustesse de la chaîne d'approvisionnement française sur le marché national et au renforcement de son offre sur les marchés internationaux.

Quelle est la vision de votre entreprise sur les attaques ciblant les fournisseurs et sous-traitants de la défense ?

MBDA MISSILE SYSTEMS MBDA France a constaté une augmentation significative du nombre de fournisseurs confrontés à un incident cyber en 2023. La tendance de 2024 est à la stabilisation sur ce haut plateau. Cependant MBDA France observe avec méfiance une baisse de la sévérité des incidents, peut-être liée au changement temporaire de cibles des groupes criminels les plus nuisibles.

Les incidents concernent majoritairement des compromissions de boites de réception des courriers électroniques, et posent surtout la question de la confidentialité d'informations sensibles. Le second type d'attaque le plus fréquemment rencontré est le rançongiciel, qui met en péril la capacité opérationnelle de notre chaîne d'approvisionnement. Ce dernier type d'incident a conduit MBDA France à réorganiser ses flux pour limiter les impacts sur la mise à disposition de nos systèmes d'armes auprès de nos clients.

Pourquoi MBDA France a-t-elle tenu à collaborer avec les autres MOI, la DGA et l'ANSSI à l'élaboration et l'application de ce référentiel de maturité cyber (RMC) ?

D'une part, le RMC est un très bel exemple de la collaboration entre industriels et autorités. La situation de départ (des initiatives industrielles ou privées pour traiter le risque cyber, non comparables ou homogènes entre elles) provoquait une multiplication des sollicitations au détriment de l'efficacité globale. La mise en place du RMC permet à tout industriel, quelle que soit sa taille, de s'évaluer suivant des critères fondamentaux et atteignables attendus de tous les donneurs d'ordres.

D'autre part, le travail nécessaire à l'évaluation ou la mise en conformité est valorisable dans des approches internationales *via* les équivalences en négociation entre le ministère des Armées et ses homologues (des États-Unis ou du Royaume-Uni par exemple).

Quels sont les attendus de MBDA France sur cette mise en application ? Quelles seraient les conséquences pour un sous-traitant qui n'aurait pas le niveau requis ?

Le déploiement du RMC n'a pour l'instant pas de dimension coercitive, sauf s'il est exigé par notre propre client (cela n'a pas encore été le cas). En revanche, MBDA France intègre systématiquement la réponse au RMC dans l'évaluation préalable à l'intégration d'une société dans le panel de fournisseurs.

Selon la relation pressentie avec la société, ou le type de matériel justifiant le lien contractuel, des restrictions peuvent donc s'appliquer. Il est également important de garder à l'esprit que MBDA est un groupe européen. Un fournisseur français intervenant sur un programme franco-britannique devra par exemple répondre aux exigences du *Ministry of Defence* britannique.
À ce titre, la conformité au RMC est un gage de fluidité dans l'approbation d'un fournisseur ou pour son utilisation sur des programmes en coopération. Enfin, le soin porté à la construction du RMC en fait aussi un outil pédagogique : il donne un support clair et reconnu qui légitime les demandes relatives à la cybersécurité.

DGA et MBDA : regards croisés sur le développement de la maturité cyber au sein de la BITD

La direction de l'industrie de défense (DID) s'inscrit pleinement dans les considérations de MBDA : le référentiel de maturité cyber de la BITD qui est le fruit d'une collaboration inédite entre les maitres d'œuvre industriels (AIRBUS, ARIANE GROUP, DASSAULT, KNDS, MBDA, NAVAL GROUP, SAFRAN, THALES) et les services de l'Etat concernés, permet d'évaluer le niveau de cybersécurité des entreprises concourantes dans la sphère défense. Il propose un référentiel unique, composé de 21 exigences pensées pour être accessibles au plus grand nombre et avec des conséquences limitées en matère d'investissements financiers et d'infrastructures.

L'atteinte du niveau « *fondamental* » du RMC ne prémunit pas contre toutes les attaques cyber mais permet d'éviter la plupart des attaques en opportunité, qui demeurent les plus fréquentes. Ce référentiel commun est une première étape essentielle dans la protection des systèmes d'information, car elle engage l'entreprise dans une dynamique positive de montée en maturité cyber et de maîtrise des risques.

C'est également, une première marche vers les exigences issues de la transposition en cours de la directive européenne *NIS 2* qui seront plus élevées que le niveau « *fondamental* » du RMC. Enfin, si ce dernier sera progressivement la référence contractuelle exigible dans le cadre des contrats de défense, il ne doit pas être perçu comme une contrainte mais comme un facteur de compétitivité sur les marchés intérieurs comme sur les marchés à l'export.

Gardons le contact

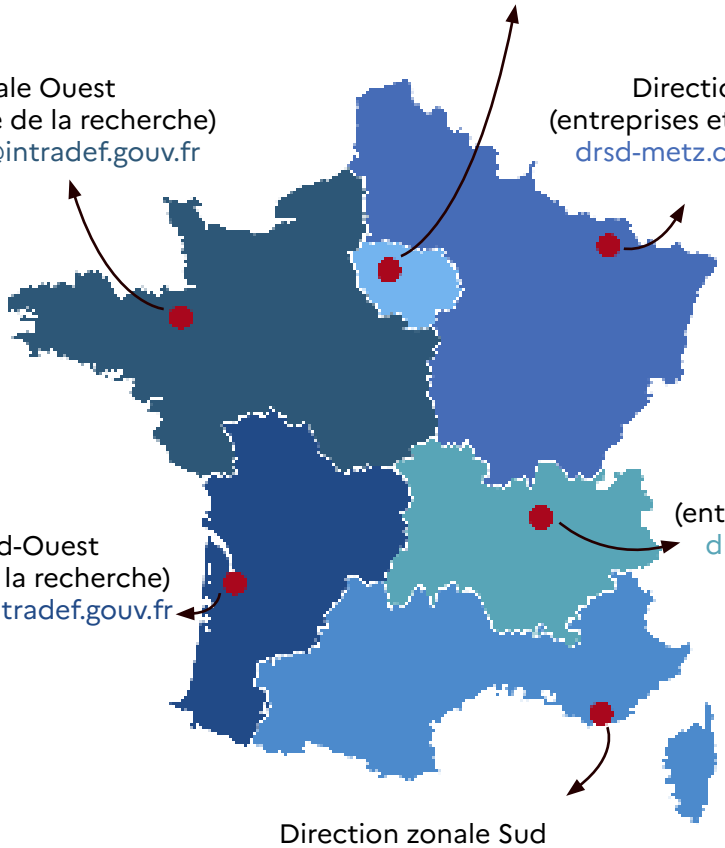
Direction centrale
Section Sensibilisation
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

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