MINISTÈRE
DES ARMÉES

Liberté
Égalité
Fraternité

Lettre d'information économique n°18
Février 2025

La BITD française après 3 ans de conflit en Ukraine

© État-major des armées / France

MOT DU DIRECTEUR

Mesdames, Messieurs,

En février 2022, dans un contexte d'accroissement des tensions internationales, l'offensive russe sur le territoire ukrainien a surpris le monde entier et précipité cette région dans un affrontement durable et de haute intensité. Trois ans plus tard, l'évolution du conflit reste dépendante du soutien politique, économique et logistique apporté par les pays occidentaux à leur allié ukrainien.

Aux côtés de ses partenaires de l'Union européenne, la France n'a cessé de soutenir l'Ukraine, en particulier par la fourniture de matériels militaires, cédés ou acquis directement par l'État ukrainien auprès des industriels de défense : canons *CAESAR* et munitions associées, véhicules de l'avant blindés (VAB), *AMX-10 RC*, missiles sol-air *MISTRAL*, missiles de croisière *SCALP*, ou encore armement air-sol modulaire (AASM), drones, etc. En complément des efforts conduits pour renforcer les capacités militaires nationales, les entreprises de la base industrielle et technologique de défense (BITD) française sont ainsi sur la première ligne d'appui aux forces ukrainiennes dans la défense de leur territoire.

En 2024, le soutien français a pris une nouvelle dimension à travers la signature d'accords de partenariats industriels qui pérennisent l'effort et conduisent à la délocalisation de certaines activités, comme la production de composants-clés et l'entretien des matériels. De même, certains industriels et consortiums français se sont réunis en « clubs » afin de renforcer leur soutien en matière de production d'armement, notamment dans des domaines d'expertise tels que les drones, l'artillerie ou encore le maintien en condition opérationnelle.

Cette aide apportée à l'Ukraine exige cependant que les entreprises de la BITD concernées s'attachent au respect strict du cadre légal du contrôle des exportations, qu'elles doivent connaitre. En outre, les acteurs de la sphère Défense sont exposés à des tentatives de déstabilisation, d'opérations d'espionnage ou d'actes de sabotages, dans les champs physique et cyber, en lien avec l'aide qu'ils apportent à l'Ukraine. Ces ingérences, au-delà de fragiliser des acteurs économiques essentiels à la BITD, portent atteinte aux intérêts fondamentaux de la Nation en affectant directement nos capacités de défense nationale.

Ainsi, la Direction du Renseignement et de la Sécurité de la Défense souhaite, à travers cette *Lettre d'information économique*, vous faire part de l'évolution des menaces susceptibles d'affecter vos entreprises dans ce contexte d'exportations sensibles. Face aux risques d'ingérences, soyez assurés que mes agents se tiennent à vos côtés pour assurer leur mission de protection, d'accompagnement et de conseil, sur le territoire national comme à l'étranger.

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

SOMMAIRE

[1] *Computer Emergency Response Team - Entreprises de Défense.*

LA RÉGLEMENTATION ET LES RISQUES ASSOCIÉS AUX EXPORTATIONS POUR LA BITD

Les exportations françaises d'armement ont atteint 8,3 milliards d'euros de prises de commandes enregistrées en 2023. À ce montant doit s'ajouter celui des commandes de biens à double usage, qui peuvent aussi avoir des applications militaires. Si ces ventes constituent une source de recettes et soutiennent la politique étrangère de la France, elles représentent également un risque juridique pour les entreprises. En effet, le non-respect du cadre législatif et des sanctions applicables en matière de contrôle des exportations font peser des risques importants sur les entreprises exportatrices.

Les matériels de guerre et biens à double usage sont soumis à des réglementations distinctes. Le dispositif de contrôle des exportations de matériels de guerre repose sur le principe général de prohibition et de dérogation. Celui-ci induit un contrôle strict de l'État sur toute la chaîne de valeur, de la production jusqu'à la vente, en France ou à l'étranger. À l'inverse, les biens à double usage peuvent être, par principe, vendus à l'étranger. Néanmoins, en fonction de leur nature et de leurs caractéristiques techniques, une licence d'exportation peut s'avérer obligatoire. Ces deux systèmes ont pour objectif de contrôler les flux sortants selon divers critères afin d'assurer la stricte conformité des opérations commerciales aux engagements internationaux de la France.

En particulier, les exportations de matériels de guerre et biens à double usage doivent respecter les sanctions en vigueur. Ces sanctions peuvent viser des personnes physiques, des personnes morales (entreprises, instituts, administrations, etc.) ou des secteurs d'activités. Elles peuvent être thématiques (ex. financement du terrorisme) ou géographiques (ex. sanctions adoptées à l'encontre de la Russie)[2].

RAPPELS SUR LES TEXTES APPLICABLES[3] :

- **matériels de guerre** : article R311-2 du code de la sécurité intérieure qui définit les différentes catégories de matériels de guerre ;
- **autorisation de fabrication, de commerce et d'intermédiation (AFCI)** : article R2332-5 du code de la défense ;
- **biens à double usage** : réglement européen UE 2021/821 qui définit les biens y compris les technologies, logiciels, le savoir-faire immatériel ou intangible – dont l'exportation est soumise à l'obtention d'une licence d'exportation ;
- **spécificité hélicoptères** : arrêté du 31 juillet 2014 qui liste les pays pour lesquels une licence d'exportation est requise ;
- **spécificité gaz lacrymogènes et agents antiémeute** : arrêté du 31 juillet 2014 ;
- **spécificité biens et technologies associés à l'ordinateur quantique** : arrêté du 2 février 2024.

[2] Rapport au Parlement 2023 sur les exportations d'armement de la France – www.defense.gouv.fr/rapport-au-parlement-2023-exportations-darmement-france.

[3] Voir LIE n°12 - *La contre-ingérence dans le contrôle des exportations de matériels de guerre* – avril 2023 – www.defense.gouv.fr/drsd/ressources-entreprises/lettre-dinformation-economique.

CAS CONCRET

Une société française commercialise des petits équipements électroniques en France. Depuis l'invasion de l'Ukraine par la Russie en 2022, la société reçoit de plus en plus de sollicitations ukrainiennes.
N'ayant jamais exporté vers un pays étranger, l'entreprise décide de faire appel à la DRSD qui l'accompagne déjà dans le cadre de ses contrats avec la Défense. Son agent de contact lui conseille de se rapprocher du Service des biens à double usage (SBDU). La société apprend ainsi que la vente de ses produits à l'étranger est soumise à l'obtention d'une licence car il s'agit de biens à double usage (BDU).

La société française dépose alors sa première demande de licence pour un de ses prospects avec l'Ukraine. Après étude de son dossier, le SBDU lui notifie un avis défavorable justifié par un risque de détournement de ses puces électroniques. Ce type de risque a fortement augmenté avec la guerre et se décline en plusieurs cas : détournement vers une application militaire non déclarée, vers un client final inconnu ou à l'honorabilité douteuse, voire vers un pays sous sanctions et/ou embargos.

En ne donnant pas suite aux sollicitations, la société française se protège des risques réputationnels et juridiques consécutifs d'une exportation.

POINTS D'ATTENTION

Pour acquérir de l'armement ou des pièces détachées destinées à la production ou au maintien en condition de vecteurs ou de systèmes d'armes, les pays soumis à un embargo (ex. Russie) peuvent mettre en place des circuits détournés. Tout exportateur doit donc se renseigner le plus exhaustivement possible sur l'honorabilité des sociétés intermédiaires ainsi que sur les destinataires finaux et accorder un soin tout particulier au circuit d'acheminement de ses exportations lors de ses prospects à l'étranger, particulièrement dans les pays à risques (Balkans, pays d'Asie centrale et d'Asie du sud-est).

RECOMMANDATIONS

Sur les vérifications préliminaires :

- ☐ désigner et former un responsable du contrôle des exportations. Celui-ci doit disposer d'un réel pouvoir décisionnel pour contrôler efficacement et protéger l'entreprise et ses dirigeants ;
- ☐ évaluer les risques relatifs à votre activité et à vos prospects ;
- ☐ former les membres de la direction et les commerciaux qui sont les premiers concernés par ces risques ;
- ☐ sensibiliser les membres du personnel aux risques induits par le commerce des armes et matériels assimilés, ainsi qu'aux risques de détournement de biens à double usage ;
- ☐ mettre en place et contrôler l'application des procédures de *due diligence* pour valider les partenariats commerciaux, les intermédiaires, etc.

Sur la conformité vis-à-vis de la réglementation :

- ☐ s'adresser aux administrations compétentes – **Direction générale de l'armement** (DGA) et **Service des biens à double usage** (SBDU) – pour toute question sur une opportunité, un classement ou le processus légal d'exportation ;
- ☐ mettre en place et appliquer des procédures afin de se conformer à toutes les étapes du contrôle des exportations, en amont (autorisation de fabrication, de commerce et d'intermédiation (AFCI), licences, etc.) et en aval (certificat de non réexportation (CNR), compte-rendu semestriel, etc.) ;
- ☐ en cas de **doute sur le classement** d'un bien, le risque de détournement ou l'opportunité d'exporter un bien à double usage : déposer un **dossier hors licence** (DHL) auprès du SBDU *via* le **portail *EGIDE*** ou par téléphone.

DES STRATÉGIES D'INGÉRENCES NUMÉRIQUES DE PLUS EN PLUS COMPLEXES

Depuis 2022, l'exposition médiatique des entreprises de la BITD française qui fournissent du matériel militaire à l'Ukraine s'est renforcée et a facilité la mise en œuvre de stratégies d'ingérences numériques de plus en plus complexes, dans les champs informationnel et cyber.

INGÉRENCES INFORMATIONNELLES :

Cette exposition médiatique augmente la vulnérabilité au risque réputationnel. Des communautés numériques d'influence qui utilisent le conflit russo-ukrainien à des fins de déstabilisation se sont développées. De ce fait, les noms des sociétés françaises qui exportent du matériel de guerre sont utilisés autant par les partisans que par les détracteurs des parties impliquées dans le conflit et peuvent devenir les cibles d'attaques informationnelles.

Plusieurs tendances se sont consolidées au cours de l'année 2024 et attestent d'une complexification des stratégies d'ingérences numériques, déployées par des acteurs malveillants à l'encontre des entreprises françaises de la sphère Défense.

La DRSD observe la constitution d'écosystèmes de désinformation qui visent à optimiser la visibilité et la diffusion de véritables offensives numériques. Ces écosystèmes reposent, d'une part, sur l'exploitation des médias, des réseaux sociaux et de la publicité. Ils ont recours, d'autre part, à des prestataires afin de développer l'infrastructure (marketing, sites internet) de ces campagnes d'influence.

La création et l'utilisation de médias, authentiques ou non, contribuent à la diffusion d'articles à charge. Ces derniers nourrissent et crédibilisent des narratifs hostiles aux intérêts de la BITD. La redondance de l'information et les citations circulaires crédibilisent ces narratifs.

Ces articles sont ensuite partagés sur les réseaux sociaux, au moyen de comptes officiels, de profils inauthentiques, de sympathisants voire d'influenceurs. Les réseaux sociaux permettent ainsi de créer une caisse de résonnance et de favoriser la diffusion de contenus viraux. Cette diffusion large peut être affinée grâce à l'acquisition d'espaces publicitaires et à la rémunération d'influenceurs, qui partagent des contenus adaptés à un public préalablement identifié.

Cette diffusion multicanaux, la redondance de l'information qu'elle suscite, la capacité à cibler des profils et à toucher une audience large visent à influencer la perception de l'auditoire pour modifier ses comportements.

CAS CONCRET

En mars 2024, une lettre appelant à l'arrêt des livraisons d'armes au profit de l'Ukraine a été distribuée au personnel d'un groupe industriel de la sphère Défense par des représentants syndicaux. Cette lettre dénonçait « *l'offensive de l'industrie de l'armement française dans l'unique but de servir le profit, les intérêts capitalistes et les guerres impérialistes* ».

Ce type de narratif, également diffusé sur les réseaux sociaux par certaines organisations syndicales, peut être amplifié à l'étranger, notamment par l'intermédiaire de médias russes adeptes de la désinformation tels que *Sputnik Afrique* et *Pravda.*

L'objectif est triple : relayer les discours critiques envers les prises de position de la France, intensifier les campagnes de dénigrement à l'encontre des entreprises françaises de Défense et inciter les salariés à se mobiliser contre leur employeur. Concrètement, pour les sociétés, une ingérence de ce type peut donner lieu à des contestations internes et des rassemblements aux abords de l'entreprise, ou encore à une perturbation de sa production et de son activité.

RECOMMANDATIONS

- ☐ réaliser une veille et être attentif aux évolutions de votre écosystème ainsi qu'à l'image ou à la réputation de votre entité, en interne, sur les réseaux sociaux et dans la presse ;
- ☐ définir et communiquer une politique de gestion de crise réputationnelle, établir un schéma de résilience[4] et préparer une communication réactive.

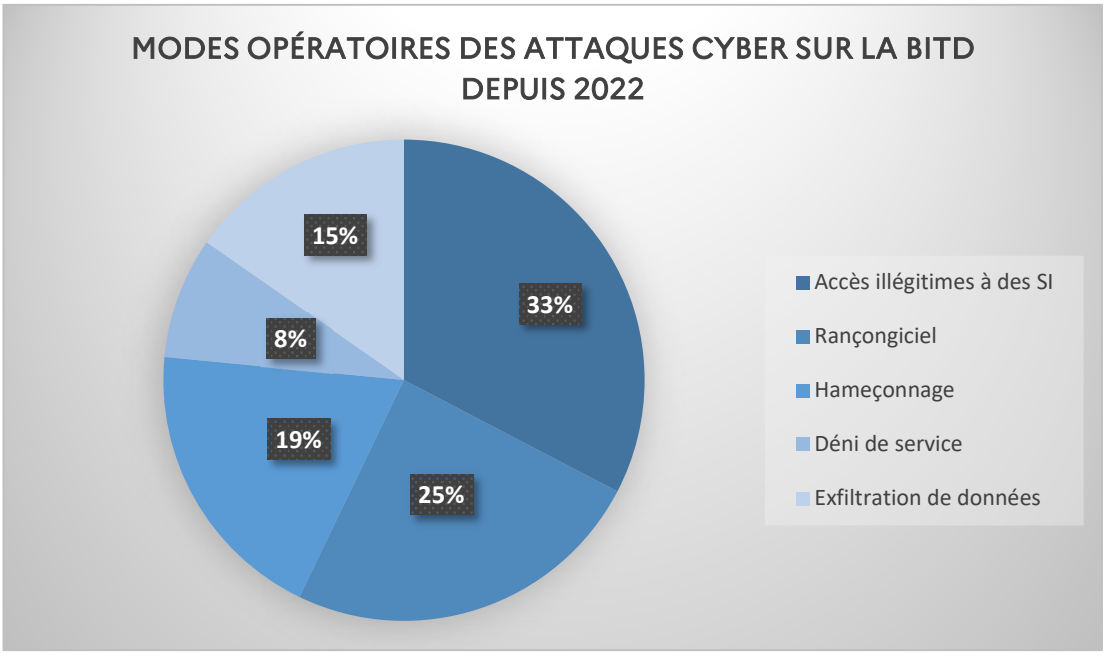
INGÉRENCES CYBER :

Depuis le début du conflit russo-ukrainien, les groupes cybercriminels pro-russes ont perpétré plusieurs cyberattaques contre des entreprises françaises appartenant à la BITD.

Ces attaques ont des conséquences variées, qui dépendent du mode opératoire utilisé (DDoS[5], rançon, etc.) ainsi que du niveau de maturité et de résilience cyber des cibles. Pour autant, dans la majorité des cas, ces actions visent le patrimoine informationnel des entreprises. Ces opérations peuvent provoquer des retards dans les activités, voire un arrêt complet de la production, avec les conséquences financières induites.

Exigeant un niveau technique avancé, les compromissions des systèmes d'information par des attaquants cybercriminels, qui déploient des rançongiciels, présentent un double risque : d'abord celui de la destruction des données pour l'entreprise, ensuite celui de leur exfiltration à fins d'exploitation par des acteurs aux motivations variées.

Lorsqu'elles sont publiées, ces données permettent parfois à un compétiteur d'accéder aux schémas d'organisation de certains programmes sensibles, voire de reconstituer l'architecture de certains composants.



[4] *Guide de survie face à la crise à l'usage des entreprises de la BITD et des agents de la DRSD* – www.defense.gouv.fr/drsd/ressources-entreprises/guides-supports-surete.

[5] Déni de service distribué.

CAS CONCRET

En 2022 et 2023, certaines entreprises de la BITD qui annonçaient des contrats avec l'Ukraine, ou dont les produits étaient livrés à l'Ukraine, ont été visées par des attaques cyber par déni de service distribué (DDoS), dans les heures qui ont suivi les communications officielles.

Les investigations de la DRSD et des services partenaires ont permis d'imputer systématiquement ces actions à des cyber activistes russophones.

Au-delà de leurs conséquences sur les systèmes d'information et le fonctionnement des entités, ces attaques peuvent générer un sentiment de vulnérabilité chez les entreprises qui en sont victimes et entacher leur réputation auprès des partenaires et des clients. Ce type d'actions engendre une résonance médiatique, complémentaire des cyberattaques, qui peut s'inscrire dans une stratégie globale combinant contre une même cible des modes d'action destinés à la déstabiliser par l'altération de ses capacités de production et l'atteinte à sa réputation.

RECOMMANDATIONS

- ☐ appliquer de manière régulière et systématique les mises à jour de sécurité ;
- ☐ vérifier que les mots de passe sont suffisamment complexes et changés régulièrement ;
- ☐ vérifier auprès de votre hébergeur que vous bénéficiez d'une protection contre les attaques DDoS, et, le cas échéant, le niveau de cette protection ;
- ☐ sensibiliser les collaborateurs aux risques cyber (hameçonnage, pièces jointes piégées, etc.) ;
- ☐ en cas de sollicitation malveillante ou de doute, contactez votre agent référent DRSD.

RESSOURCES

- **ANSSI :** Guide – *Comprendre et anticiper les attaques DDoS*[6] ;
- **Cybermalveillance :** *Attaque DDoS, que faire.*[7]

[6] www.cyber.gouv.fr/publications/comprendre-et-anticiper-les-attaques-ddos
[7] www.cybermalveillance.gouv.fr/tous-nos-contenus/fiches-reflexes/attaque-en-deni-de-service-ddos

LE CERT [ED] – CENTRE DE RÉPONSE À INCIDENT AU PROFIT DES ENTITÉS DE LA SPHÈRE DÉFENSE

Le CERT [ED] contribue à la prévention des incidents de sécurité informatique, à l'analyse et au partage de l'information d'intérêt cyber pour le secteur des entreprises de Défense et à la coordination de la réponse aux incidents ciblant ce secteur, en coopération et coordination avec les acteurs régionaux ou nationaux de la cybersécurité.

SES MISSIONS

- sensibiliser aux risques cyber : le CERT [ED] partage ses connaissances et son expérience en sensibilisant les entreprises de Défense ;
- effectuer une veille des vulnérabilités : le CERT [ED] contribue à réduire le risque d'attaques informatiques en communiquant, sur demande, les vulnérabilités logicielles ou matérielles du système considéré;
- répondre aux incidents de sécurité informatique : le CERT[ED] accompagne les entreprises du secteur de la Défense victimes d'incidents de sécurité ;
- coordonner / coopérer : le CERT[ED] agit, pour le secteur de la Défense, avec les acteurs régionaux et nationaux de la cybersécurité.

LES ENJEUX DE L'INDUSTRIE DE DÉFENSE

La transformation numérique :

- transition d'ampleur (technologies de l'information et de la communication, technologies opérationnelles en système industriels de production) qui induit une augmentation de la surface vulnérable aux attaques ;
- utilisation mixte des équipements professionnels et privés ;
- faible intérêt pour la culture de la sécurité et l'hygiène informatiques ;
- organisations des TPE, PME et ETI qui intègrent moins la sécurité informatique ;
- complexification réglementaire.

Pour ces raisons, les sous-traitants de petite taille des grandes industries de Défense, détenant des « actifs » de valeur (ou *assets*), sont devenus des cibles privilégiées des attaquants de la *supply-chain*.

Les difficultés inhérentes :

- appréhension partielle du risque cyber ;
- manque de solutions « clés en main » ;
- coût dissuasif de la sécurité numérique ;
- perte de maîtrise de l'infrastructure SI.

Les multiples facettes du risque cyber :

- *conséquences financières* : préjudice direct (matériel, humain, financier) ou indirect (baisse du chiffre d'affaires) ;
- *effets sur l'image et la réputation* : image de marque entachée, perte d'appels d'offres, diminution des ventes ;
- *atteintes au patrimoine intangible* : vol de propriété intellectuelle, développement de concurrents ;
- *fragilisation du capital humain* : stress, débauchages, perte de confiance ;
- *non-conformité* : amendes, sanctions (non respect du RGPD).

Pour signaler un incident de sécurité ou nous informer d'une menace :

0 805 046 300 (appel gratuit) - **cert-drsd.contact@def.gouv.fr**

LA NÉCESSITÉ D'UNE VIGILANCE ACCRUE FACE À LA MENACE DE SABOTAGE

Depuis le début de la guerre en Ukraine, les entreprises de Défense sont soumises à une menace accrue d'origine humaine pouvant cibler leurs savoir-faire et leurs emprises. Face à celle-ci, la protection et la sécurité des installations de la BITD constituent deux préalables à la continuité de l'activité de production d'armement.

S'il n'y a pas eu de conséquence majeure pour l'activité des entreprises visées par des actes de sabotages, et si leur origine ne peut pas être directement reliée à leur production au profit de l'Ukraine, ces sociétés ne sont pas moins susceptibles d'être visées directement. Elles peuvent également subir les conséquences d'un acte de sabotage contre un tiers (sabotage indirect). Cela peut être le cas notamment des actions menées à l'encontre des réseaux d'approvisionnement électrique.

Pour prévenir une atteinte à votre outil de production, la DRSD vous accompagne et vous conseille quant aux investissements à consentir en termes de protection, en identifiant les vulnérabilités de vos emprises. En tout état de cause, il vous est recommandé de signaler au Service tout incident ou tentative d'actes malveillants et de déposer systématiquement une plainte auprès des forces de sécurité intérieure (Gendarmerie et Police).

CAS CONCRET

Après avoir reçu des menaces par courrier et courriel, une société française qui fabrique et exporte du matériel militaire vers l'Ukraine a été victime d'une intrusion avec découpe du grillage périphérique durant l'été 2024.

La même nuit, la société a subi quatre jets de cocktails *Molotov*. S'il n'y a pas eu de conséquence sur la capacité opérationnelle du site (un seul des quatre dispositifs incendiaires a fonctionné), il ne peut cependant pas être exclu que l'objectif de cette intrusion était de causer le maximum de dommages possibles, en incendiant l'ensemble du bâtiment.

Dans les semaines qui ont suivi cet incident, des survols de drones ont été détectés à plusieurs reprises par les agents de sécurité. Accompagnée et conseillée par un agent de la DRSD, la société a rapidement déposé plainte à la suite de chacun de ces incidents.

RECOMMANDATIONS

- ☐ former votre personnel au signalement auprès de votre chaîne de sécurité de toute situation anormale (regroupements en périphérie du site, comportements douteux, etc.);
- ☐ informer votre agent référent de la DRSD et la Gendarmerie ou la Police de tout incident ou événement suspect concernant la protection et la sécurité de vos installations.

L'ACCOMPAGNEMENT DE LA DRSD AU PROFIT DES INDUSTRIELS FRANÇAIS EN EUROPE DE L'EST

Dans sa mission de protection au profit de la BITD, la DRSD accompagne les entités de la sphère Défense qui souhaitent devenir fournisseurs d'États étrangers. À cette fin, des détachements du Service sont désormais déployés en permanence dans trois capitales d'Europe de l'Est : **Bucarest** (Roumanie), **Tallinn** (Estonie) et **Varsovie** (Pologne). Dotés d'une compétence régionale, les agents qui les composent sont en mesure de se déplacer dans les différents pays de la zone.

En lien constant avec les autorités locales, avec lesquelles ils interagissent de manière transparente, les détachements du Service à l'étranger sont, au quotidien, au service des forces comme des entreprises françaises de Défense.

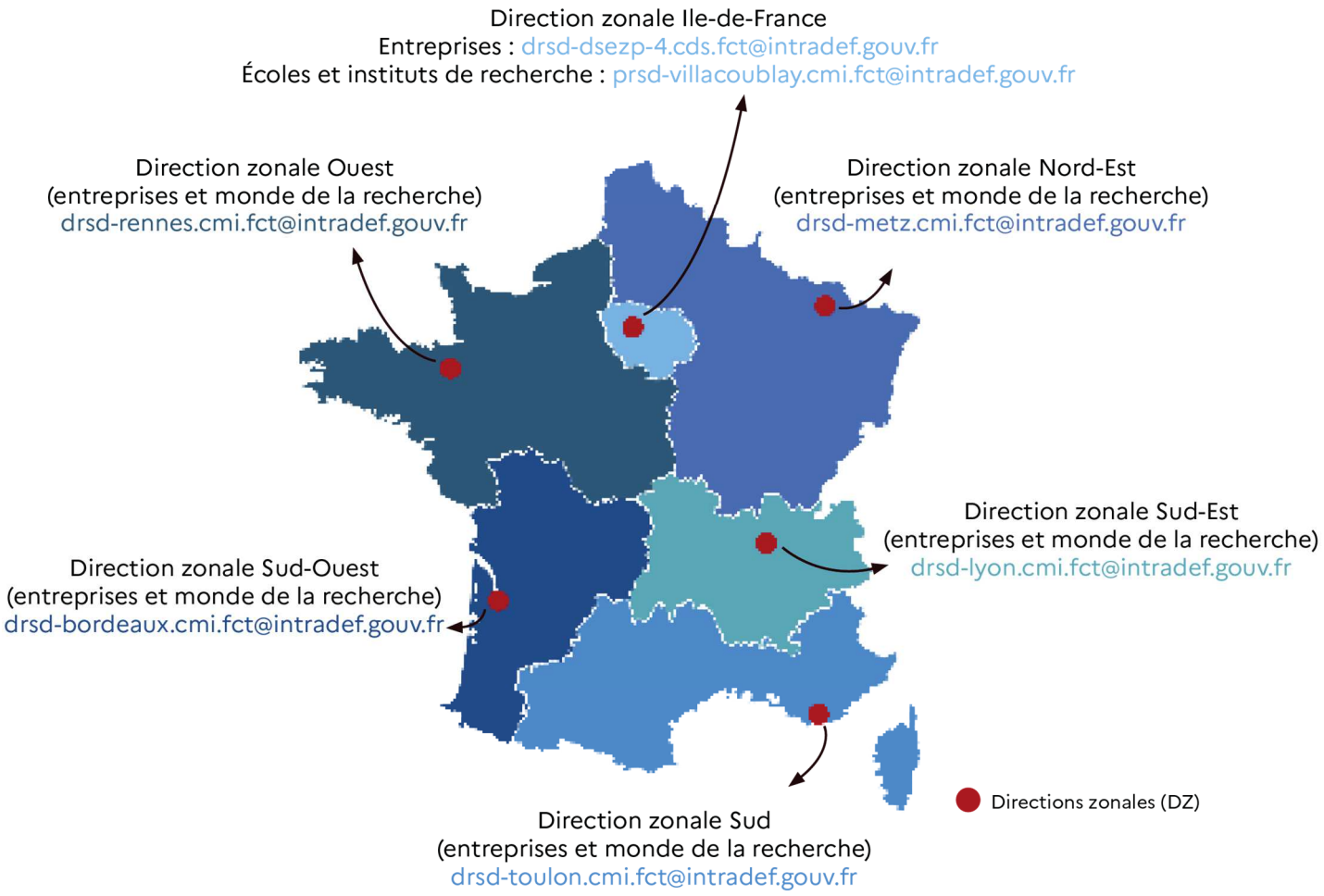
Ainsi, n'hésitez pas à contacter votre correspondant DRSD habituel qui fera le lien avec nos détachements sur place, ou directement notre direction zonale Hors-Métropole (drsd-dzhm.cmi.fct@intradef.gouv.fr), qui pourra vous accompagner lorsque que vous envisagerez des projets ou marchés d'exportations dans cette région.

Par ailleurs, le Service remercie les sociétés qui se sont déjà rendues dans la zone dans le cadre de contrats avec l'Ukraine pour le retour d'expérience (RETEX) qu'elles voudront bien partager, dans le but de favoriser la diffusion des bonnes pratiques et une évaluation des risques toujours plus affinée.

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



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