LIE n°15 de la DRSD

UKRAINE – 2 ans après, état des lieux des risques d'ingérences visant la BITD française

La lettre d'information économique
Janvier 2024

Sommaire

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

Mesdames, Messieurs,

Le 24 février 2022, les forces armées russes envahissaient l'Ukraine huit ans après l'annexion de la Crimée. Cette invasion est à ce jour la plus importante opération militaire sur le sol européen depuis la fin de la Seconde Guerre mondiale.

La première année du conflit a été marquée par un envoi massif de matériels militaires vers l'Ukraine. La deuxième année du conflit a témoigné de l'accélération du besoin de coopération industrielle entre l'Ukraine et les pays occidentaux.

Une nouvelle dynamique voit le jour avec l'établissement de partenariats entre les entreprises françaises et ukrainiennes afin de développer puis de pérenniser la base industrielle et technologique (BITD) de défense du pays. Promue par le gouvernement ukrainien, cette dynamique répond à deux objectifs : créer localement des sites de production à même de fournir l'effort de guerre attendu et être en mesure d'effectuer sur place le maintien en condition opérationnelle des matériels précédemment livrés.

Dans ce contexte d'économie de guerre, le maintien des capacités opérationnelles de notre outil de défense pour notre propre protection doit aussi et surtout guider notre action. Or, les sollicitations croissantes auxquelles font face les entreprises françaises amplifient les risques d'opérations d'espionnage ou d'actions de sabotage ainsi que les tentatives d'ingérences, notamment dans le cyberespace.

Pleinement consciente des conséquences induites par ces enjeux, la Direction du Renseignement et de la Sécurité de la Défense souhaite, à travers cette lettre d'information économique, partager avec vous un panorama mis à jour des risques et des menaces pesant sur les entreprises de la BITD française dans le cadre du conflit russo-ukrainien.

Au seuil de cette nouvelle année, je vous adresse mes vœux les plus chaleureux et renouvelle à ce titre notre engagement à concourir à votre protection sur le territoire national et sur les marchés à l'étranger. Soyez assurés de l'engagement de nos agents dans notre action collective d'anticipation de ces nouvelles menaces.

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

Sanctions internationales et *compliance* : les risques liés au *lawfare*

Les sanctions adoptées par les pays occidentaux en réaction au **conflit russo-ukrainien** induisent des responsabilités supplémentaires en matière de conformité pour les industriels français.

Ainsi, les entreprises de la BITD sont amenées à mettre en œuvre au sein de leurs structures un travail complexe de **veille**, d'**analyse** et de **conformité** aux sanctions. Les entreprises intégrées dans des chaînes de production sont également appelées à veiller à la conformité de **leurs partenaires et sous-traitants**, qui peuvent être à l'origine du détournement de composants vers des entités sanctionnées.

Au-delà des risques liés à l'exportation, les entreprises de défense françaises commercialement actives dans la zone doivent porter une attention particulière aux **problématiques de corruption**, particulièrement médiatisées en Ukraine depuis le début de l'année 2023.

Au regard de ces exigences légales et de la responsabilité induite, les entreprises peuvent également faire l'objet d'une **surveillance renforcée**. À titre d'exemple, les autorités américaines ont mis en place une *task force « Kleptocaptur »* en mars 2022 dans le but de veiller à la bonne application des sanctions américaines visant les oligarques russes. Composée de fonctionnaires issus de différentes agences américaines, dont le *Federal Bureau of Investigation* (FBI), cette équipe s'intéresse notamment à la conformité des entreprises européennes aux sanctions américaines.

En outre, les contrôles effectués lors des **délivrances de licences d'exportation** par les administrations étrangères sont susceptibles d'être renforcés pour mieux prendre en compte les risques de détournement de matériel vers la Russie.

CAS CONCRET

Contexte : en 2022, conformément aux sanctions en vigueur, un industriel français a interrompu son partenariat avec un consortium étranger, dans lequel était impliquée une société sous-traitante russe visée par des sanctions. Un an plus tard, l'entreprise française a envisagé de relancer la coopération compte tenu du potentiel rachat par ce consortium du programme et des brevets détenus par la société russe. Ce consortium devait également maintenir en poste le personnel employé par la société russe.

Risques : si ce rachat peut donner l'impression d'écarter le risque induit par la présence d'une société russe, l'incertitude sur les liens financiers persistants entre la société russe et le consortium est susceptible de mettre l'industriel français en difficulté.

Sanctions internationales et *compliance* : les risques liés au *lawfare*

CAS CONCRET

Contexte : en mars 2022, une administration étrangère a directement sollicité un industriel français pour lui demander d'identifier les produits qui auraient pu être vendus à une liste de personnes physiques et morales visées par les sanctions contre la Russie. Sans consulter l'administration française, l'entreprise a transmis les informations demandées pour prouver sa bonne foi à l'autorité étrangère.

Risques : le Service ne peut exclure que ces documents aient pu contenir des éléments incriminants, susceptibles d'engendrer ensuite des poursuites étrangères judiciaires ou administratives.

Recommandations

- ☐ Engager des procédures robustes de ***due diligence***[1] avant d'entrer en relation contractuelle avec un tiers pour écarter tout risque de flux financier vers une entité sanctionnée ;
- ☐ Renforcer les compétences de l'entreprise en matière de conformité, notamment pour veiller au **respect des sanctions internationales** et pour assurer un **suivi des réexportations** des produits de l'entreprise par ses clients ;
- ☐ **Contacter vos référents locaux de l'administration française** (DISSE, DGA, DRSD) en cas de demande d'information en provenance d'une autorité étrangère.

- **Pour aller plus loin, consulter :**
  - **la LIE n°14 « Le *lawfare* ou l'usage du droit à des fins stratégiques »**
  - **la LIE n°12 « La contre-ingérence dans le contrôle des exportations de matériels de guerre »**.

[1] Source Lexis Nexis : la *due diligence* est un concept emprunté à la jurisprudence des Etats-Unis que l'on utilise en France dans le contexte du droit des achats. Dans la langue française, on parle d'obligation de vigilance, mais l'expression anglaise tend à se généraliser, en raison de sa spécificité juridique. La *dilligence*, qu'elle soit raisonnable ou renforcée, renvoie à l'obligation pour l'acheteur d'être vigilant, selon le principe du *caveat emptor*. Son but est de sécuriser achats et transactions.

Dissémination et intermédiations illicites : les risques liés aux détournements de matériels de guerre et de biens à double usage

RISQUES DE DISSÉMINATION ET DE DÉTOURNEMENT DE MATÉRIELS DE GUERRE ET DE BIENS À DOUBLE USAGE

Le conflit russo-ukrainien a été marqué par des envois massifs de matériel de protection (casques, gilets-pare-balles, etc.) et de matériel létal (artillerie, munitions, etc.). Il a aussi mis en lumière l'enjeu primordial que représente l'usage militaire intensif des drones.

Dans ce contexte, les sociétés françaises sont régulièrement sollicitées pour l'envoi de pièces de rechange ou de composants liés à des matériels précédemment livrés. En effet, l'Ukraine souhaite effectuer les réparations et la remise en condition des matériels endommagés par ses propres moyens. Les sociétés françaises sont ainsi de plus en plus souvent approchées pour la fourniture de biens à double usage, à savoir de matériels pouvant être utilisés pour des applications duales, tant civiles que militaires.

Ce faisant, elles peuvent se trouver exposées à un risque de détournement de leurs exportations pour des utilisations et/ou vers des utilisateurs non déclarés.

RISQUES LIÉS AUX INTERMÉDIATIONS DOUTEUSES

Les entreprises françaises amenées à traiter « de gré à gré » avec les entreprises ukrainiennes ne disposent pas nécessairement d'un accès direct aux besoins exprimés par leurs homologues. Cette contrainte tend à renforcer le rôle des intermédiaires sur le marché ukrainien.

La contractualisation avec ces acteurs engendre trois risques principaux :

1. **Un risque économique** : implication dans des rétro-commissions ou des schémas de corruption, perte ou rupture de contrat pour la société, transgression de restrictions commerciales à l'encontre de certains pays (sanctions internationales et/ou embargos) ;

2. **Un risque de vol et de dissémination[2] du matériel pendant ou après la livraison** : manque de transparence de l'intermédiaire sur le destinataire final, détournement du matériel, implication dans des trafics d'armes en lien avec la criminalité organisée ;

3. **Une atteinte à l'image de l'entreprise** résultant de ces deux premiers risques.

[2] La dissémination se définit comme le fait de voir un armement conventionnel tomber aux mains d'un utilisateur final ne correspondant plus à l'acquéreur prévu.

Dissémination et intermédiations illicites : les risques liés aux détournements de matériels de guerre et de biens à double usage

CAS CONCRET

Contexte : une société française fabriquant des munitions est sollicitée par un intermédiaire au profit d'un conglomérat de défense ukrainien. D'après l'intermédiaire, le marché financièrement lucratif pour la société munitionnaire doit être signé rapidement avant que cette opportunité commerciale ne lui échappe.

Faits : celle-ci exporte donc les munitions, sans attendre l'acceptation de la demande de licence d'exportation par l'administration française. L'entreprise informe finalement son agent référent DRSD de leur envoi un mois plus tard.

Risques : après investigations, il apparait que l'intermédiaire est défavorablement connu du Service et que le conglomérat de défense ukrainien est identifié pour avoir été impliqué dans une affaire de dissémination d'armements. De plus, peu de temps après l'exportation de ces munitions sans autorisation de l'État, l'utilisation de ces dernières a été détectée dans un conflit en Afrique.

Impact : les conséquences pour la société française sont doubles : d'une part, la suspension par la commission interministérielle pour l'étude des exportations de matériel de guerre (CIEEMG) des licences d'exportations précédemment accordées par cette dernière à l'entreprise. D'autre part, pour l'entreprise, la perte immédiate de plusieurs contrats déjà signés ou en cours et la mise en cause de la société dans plusieurs articles de presse.

CAS CONCRET

Contexte : une société française spécialisée dans la conception de drones est approchée par un apporteur d'affaires français, inconnu de son service commercial. Il expose un projet de coopération industrielle sur le territoire ukrainien, en proposant ses services pour une mise en relation avec une entreprise locale.

La société française, souhaitant obtenir le marché, est sollicitée pour fournir des informations sur ses capacités industrielles à l'apporteur d'affaires, celui-ci se proposant de les présenter aux autorités locales.

La société prévient son agent référent DRSD de cette approche et de sa volonté de développer son activité commerciale vers l'Ukraine.

Mesures : l'agent déconseille à l'entreprise de poursuivre les démarches avec cet intermédiaire. En effet, ce dernier est défavorablement connu du Service pour des faits de corruption lors d'un marché précédent ayant mis en difficulté une société de défense française.
Finalement, la société rompt tout contact avec l'intermédiaire avant même de lui avoir versé un acompte et de lui avoir transmis des informations sensibles.

Recommandations

- ☐ Mettre en place des procédures de contrôle des exportations comportant une vérification appropriée de l'honorabilité des utilisateurs finaux et des éventuels intermédiaires.
- ☐ Ne pas faire confiance d'emblée à des intermédiaires dont l'honorabilité n'est pas clairement établie. En cas de doute, s'adresser à votre référent DRSD.
- ☐ Se tourner vers les **administrations compétentes**, la **Direction générale de l'armement** du ministère des Armées (DGA) ou le **Service des biens à double usage** du ministère de l'Économie, des Finances et de la Souveraineté industrielle et numérique (SBDU) pour toute question sur une opportunité d'exportation.

Dans le cas d'un « bien à double usage » :

- ☐ En cas de doute sur le statut de « bien à double usage » d'un produit, déposer une **demande hors licence** (DHL) auprès du Service des biens à double usage (SBDU/MEFSIN), via le portail EGIDE ou par téléphone, pour s'enquérir de la faisabilité d'un projet d'exportation.

Dans le cas d'un « matériel de guerre » :

- ☐ Mettre en place et appliquer des procédures pour se conformer à toutes les étapes du contrôle d'exportation, de l'amont [*autorisation de fabrication, de commerce et d'intermédiation (AFCI), licences d'exportation, etc.*] à l'aval [*Certificat de non-réexportation (CNR), comptes rendus semestriels, contrôle a posteriori (CMCAP) etc.*].

- **Pour aller plus loin, consulter la LIE n°12 « La contre-ingérence dans le contrôle des exportations de matériels de guerre ».**

Déplacements et négociations : des périodes à risques

VIGILANCE À L'OCCASION DES DÉPLACEMENTS ET NÉGOCIATIONS

Les livraisons de matériels français en Ukraine et les premiers accords visant à mettre en place des lignes de production sur le territoire ukrainien obéissent à des logiques d'efficacité mais augmentent les risques d'ingérences.

En effet, des acteurs ukrainiens malveillants isolés, souhaitant profiter de la coopération franco-ukrainienne, peuvent tenter de capter des informations sensibles.

Aussi, les services russes peuvent chercher à obtenir des informations répondant aux intérêts de leurs autorités ou conduire des actions de sabotage sur les matériels d'origine occidentale mis en œuvre par les forces ukrainiennes. Ces tentatives peuvent notamment passer par l'infiltration des lignes de production. La Russie peut à cette fin utiliser ses services de renseignement ainsi que des entreprises agissant sous faux pavillon, voire recruter spécifiquement des agents de circonstance.

Les captations d'informations peuvent revêtir plusieurs formes.

Lors des négociations, les modes opératoires permettant d'obtenir des informations sur la stratégie d'une entreprise ou sur des savoir-faire particuliers reposent sur :

- l'approche des employés, notamment par le biais des réseaux sociaux ou à la suite d'une invitation à des « conférences » tous frais payés par certaines délégations étrangères ;
- la remise d'un cadeau piégé (équipement électronique ou numérique) ;
- le vol ciblé de supports et matériels informatiques malgré leur chiffrement, maquillé en vol d'opportunité ;
- la copie du contenu de supports informatiques lors des passages en douanes ou dans tout lieu où ils seraient laissés sans surveillance (chambres d'hôtels, restaurants, etc.) ;
- les prises de vue (photographies et vidéos) et captations sonores lors de réunions de travail ;
- la récupération d'informations stratégiques lors d'audits externes.

Une fois le matériel livré, le plus grand risque réside dans le *retro-engineering* (ou « ingénierie inverse ») : les armées et services russes cherchent à s'emparer de certains matériels afin d'améliorer leurs propres systèmes.

Pour ces raisons, il est impératif de faire remonter à la DRSD tout comportement anormal de la part de vos clients ou de vos collaborateurs. Les services de renseignement russes ainsi que certains acteurs malveillants présents sur le sol ukrainien peuvent déployer des moyens conséquents pour s'emparer des données ou des technologies des entreprises occidentales s'ils estiment qu'elles représentent un intérêt significatif.

Déplacements et négociations : des périodes à risques

CAS CONCRET

Contexte : une entreprise française a été contactée par un intermédiaire ukrainien qui affirmait vouloir livrer un système d'armes aux forces armées ukrainiennes. Alors que les négociations étaient engagées et à la suite de déplacements de délégations en France puis en Ukraine, plusieurs ordinateurs appartenant à l'entreprise française ont disparu. Chaque vol présentait les caractéristiques d'un acte de simple délinquance.

Pourtant, à la suite de ces évènements, les interlocuteurs ukrainiens de la société ont semblé de moins en moins enclins à poursuivre les négociations pour finalement y mettre un terme.

Conséquences : peu de temps après, une entreprise ukrainienne a annoncé la mise en production d'un matériel équivalent. A la suite de cet incident, le gouvernement ukrainien a pris des mesures à l'encontre de l'intermédiaire et de l'entreprise malveillante.

Faites part de vos étonnements !

- Si vous constatez lors d'une visite de délégation ou d'une négociation, l'attitude insistante d'un personnel qui tente de se rapprocher de vous, de vous offrir des cadeaux, il peut s'agir d'une approche en vue de capter certaines informations.
- Si vous êtes questionné sur des briques technologiques sensibles ou sur des retards technologiques, faites remonter ces sollicitations singulières à la DRSD. D'autres entreprises pourraient être concernées ;
- Si vous recevez des délégations étrangères, informez votre agent référent en amont de la visite. Relevez le plus d'informations possibles (nom, prénom, poste occupé, numéro de téléphone, adresse email, etc.) sur leurs membres et soyez stricts sur le respect de la liste des participants. Ces informations serviront à protéger les entreprises dans le cas où elles feraient l'objet d'approches à des fins concurrentielles, d'espionnage ou d'atteintes de vos capacités de production.

Une menace protéiforme : les risques d'ingérences informationnelles

Dans le contexte actuel d'économie de guerre, les rapports de force se jouent également dans le champ de l'influence où la maîtrise de l'information est un enjeu majeur pour les États, les belligérants et les concurrents. Ainsi, les entreprises de la BITD impliquées sur le marché ukrainien sont particulièrement exposées à des risques d'ingérences informationnelles.

La facilité d'accès à l'information, notamment par l'essor des réseaux sociaux offre la capacité de formuler et diffuser une opinion sur un évènement ou une situation. L'effet « *buzz* » d'une publication sur les réseaux sociaux peut déclencher un séisme réputationnel et entacher l'image d'une entreprise. Or, les sujets liés à la défense présentent un caractère fédérateur et mobilisateur, à fort potentiel de viralité et peuvent perturber l'activité d'une entité. L'industrie de défense française doit ainsi se protéger face aux *fake news*, aux manœuvres de désinformation et de manipulation de l'information, qui sont autant de moyens de déstabilisation utilisés par la société civile ou par des acteurs étatiques, paraétatiques ou économiques.

CAS CONCRET

Contexte : une association pro-russe organise des manifestations devant les usines d'un industriel français afin de condamner la fourniture prochaine de matériel de guerre à l'Ukraine et son emploi potentiel contre des civils.

Conséquences : malgré une faible mobilisation locale, ces événements sont illustrés par des images laissant croire à une participation importante et sont relayés par la presse, repris et surtout amplifiés bien au-delà de leur portée réelle par des médias russes et étrangers à des fins de désinformation.

CAS CONCRET

Contexte : un journaliste prend contact avec une entreprise de la BITD dans le but d'obtenir des réponses sur le type, les capacités et la criticité du matériel fourni à l'Ukraine.

Conséquences : cette approche sous couvert de la rédaction d'un article peut représenter un risque d'atteinte réputationnelle pour la société si elle y donne suite. En effet, les informations obtenues pourraient être réutilisées pour développer un narratif anti-français. Par ailleurs, l'instrumentalisation du journaliste par la Russie est un mode d'action régulièrement identifié.

Recommandations

- ☐ Établir une charte du bon usage des médias sociaux et informer les collaborateurs quant aux risques inhérents à leur utilisation.
- ☐ Être attentif aux évolutions de votre écosystème et à ce qui est dit de votre entité sur les réseaux sociaux et dans la presse.
- ☐ Définir une politique de gestion de crise réputationnelle et établir un schéma de résilience.

Hameçonnage et attaques DDOS : la persistance de la menace cybernétique

LA MAÎTRISE DU CYBERESPACE : NOUVEAU CHAMP DE BATAILLE DÉTERMINANT POUR REMPORTER LA GUERRE

Dans le cadre de la crise russo-ukrainienne, plusieurs groupes cyber-partisans pro-russes se sont développés durant les premiers mois du conflit. Cet écosystème protéiforme s'est fortement structuré durant l'année 2023 autour de grands groupes tels que *KillNet, Cyber Army of Russia Reborn* ou encore *Anonymous Soudan*.

Des attaques par déni de service distribué corrélées aux livraisons d'armement en Ukraine

Ces groupes réalisent principalement des attaques par déni de service distribué (DDoS - *Distributed Denial of Service*)[3] sur des cibles occidentales afin d'alimenter des scénarios informationnels pro-russes.

Comme d'autres États alliés de l'Ukraine, la France est l'une des cibles principales de ces groupes, avec plusieurs centaines d'attaques DDoS recensées depuis le début du conflit. Le Service a observé des attaques ciblant plusieurs entreprises de la BITD immédiatement après l'annonce d'exportations d'équipements au profit de l'Ukraine. Portant essentiellement atteinte à l'image des sociétés visées, ces attaques ne durent généralement que quelques heures et n'ont eu jusqu'à présent qu'un faible impact opérationnel sur l'activité des entreprises concernées.

Un volume constant de tentatives d'hameçonnage

Le Service observe, sur le périmètre des entreprises de la BITD, un flux continu de tentatives de compromission par hameçonnage. Leur objectif est de gagner un accès sur les systèmes informatiques des entreprises victimes. L'hameçonnage reste le principal vecteur d'infection. Aucune campagne de ce type spécifiquement liée au conflit russo-ukrainien n'a été observée par le Service sur son périmètre, cependant l'intensification des relations industrielles entre la France et l'Ukraine pourrait être utilisée par des acteurs malveillants pour conduire des attaques à l'encontre de la BITD.

La menace des *wipers*

Le Service n'a pas observé d'attaque porteuse de codes malveillants de sabotage (*wiper*). Utilisé à l'encontre d'entités ukrainiennes notamment en début de conflit, ce mode opératoire pourrait cependant apparaître au sein de la BITD dans le cadre de l'intensification des relations industrielles franco-ukrainiennes.

La menace des rançongiciels

Les attaques par rançongiciel menées par des groupes principalement russophones tels que *REVIL*, *Lockbit3.0* ou *RagnarLocker*, continuent de cibler par opportunité des entreprises de la BITD.

[3] 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.

Hameçonnage et attaques DDOS : la persistance de la menace cybernétique

Ces attaques peuvent avoir pour conséquences :

- d'une part, un fort impact sur l'activité entrainant une interruption du fonctionnement des systèmes d'information de l'entreprise engendrant des retards de production ;
- d'autre part, des fuites de données liées au patrimoine industriel de l'entreprise. Dans 55 % des incidents recensés par le Service, une exfiltration de données est observée lorsque l'attaquant parvient à pénétrer le réseau d'une entreprise. Un nombre important de ces exfiltrations donne ensuite lieu à une publication en ligne dans le cadre d'une manœuvre de rançonnage, voire à la revente en ligne sur le *dark web* de données monnayables.

CAS CONCRET

Une attaque par rançongiciel contre une entreprise de la BITD

Contexte : à la suite de son annonce d'envoi de matériel en Ukraine, une entreprise de la BITD est victime d'une attaque par rançongiciel de grande envergure.

Conséquences : cette cyberattaque entraine un arrêt complet de son activité pendant plusieurs semaines. L'entreprise ne disposant pas de sauvegardes sanctuarisées de ses systèmes, les conséquences de cette attaque engendrent une perte quasi-complète de son patrimoine numérique entrainant des retards industriels et une perte de savoir-faire sur son activité.

CAS CONCRET

Revendication de fuite de données contre une entreprise de la BITD

Contexte : un groupe de cyberattaquants procédant par rançongiciel revendique une exfiltration de données à l'encontre d'une entreprise de la BITD, en réaction à son implication dans le conflit russo-ukrainien.

Conséquences : 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.

Hameçonnage et attaques DDOS : la persistance de la menace cybernétique

RAPPEL : LE *CERT [ED]* SE TIENT À VOS CÔTÉS

CERT [ED]

0 805 046 300

Réponse à incident

Parmi ses missions stratégiques, le CERT ENTREPRISES DE DÉFENSE ou *CERT [ED]* apporte **assistance et conseil aux entreprises pour la caractérisation et la gestion des incidents**.

Face aux campagnes d'hameçonnage toujours plus importantes ciblant le secteur de la défense depuis le début du conflit russo-ukrainien, le *CERT [ED]* apporte son soutien aux entreprises de défense. Les groupes cybercriminels ciblent aujourd'hui en priorité des entités de la *supply chain* qui est couverte pour le secteur de la défense par le *CERT [ED]* dans le cadre de sa mission de protection.

La mise en œuvre de nouveaux *malwares* de la famille des « *infostealer* » par des acteurs cybercriminels (méthode d'accès initiale concurrente à l'hameçonnage) offre aux attaquants des points d'entrée facile dans les entreprises. Le *CERT [ED]* apporte ainsi son expertise dans les recommandations d'emploi des moyens numériques, notamment sur le cloisonnement de l'utilisation des ordinateurs/téléphones professionnels et privés.

Enfin, face à des acteurs cybermalveillants, tels que *NoName057* apparu au début du conflit russo-ukrainien et spécialisé dans les attaques DDoS ou encore *LockBit* plus connu pour ces rançongiciels et dont les attaques ont redoublé ces derniers mois, le *CERT [ED]* accompagne les entreprises dans la réponse à incidents en les conseillant sur les mesures d'urgence et les bonnes pratiques pour limiter les conséquences de l'incident cyber.

Synthèse des risques et recommandations

LES RISQUES

AVANT

Risque de captation de savoirs et de savoir-faire : lors de déplacements ou des visites non-maîtrisées de délégations étrangères

Risque cybernétique avec déni de service et rançongiciel

Risque réputationnel avec campagnes de désinformation

PENDANT

Risque de captation de savoirs et de savoir-faire : lors de déplacements ou des visites non-maîtrisées de délégations étrangères

Risque de captation de savoirs et de savoir-faire : lors de la production, du montage et du maintien en condition opérationnelle

Risque de sabotage

Risque de dissémination ou de prolifération de matériel avec atteinte à l'image de l'entreprise

APRES

Risque juridique lors du montage contractuel (FCPA, ITAR, EAR)

Risque économique et juridique provoqué par intermédiations douteuses

Risque de captation de savoirs et de savoir-faire : lors de déplacements ou des visites non-maîtrisées de délégations étrangères

Risque de rétro-ingénierie des matériels prêtés ou vendus

LES RECOMMANDATIONS

AVANT

Mettre en place une veille réputationnelle sur son entreprise

Alertez votre chaîne sécurité et votre agent DRSD en cas de volonté de développer des relations commerciales avec l'Ukraine

PENDANT

Informer la chaîne DRSD de tout déplacement, visite de délégation étrangère

Veiller à la conformité juridique de ses sous-traitants et fournisseurs

Mettre en place un processus de contrôle des exportations

Mise à jour des paramètres SI et système robuste cyber

Sensibiliser les collaborateurs aux bonnes pratiques d'hygiène informatique

APRES

Systématiser le rapport d'étonnement

Assurer un suivi des réexportations de vos produits le cas échéant

Remontez toute information à la chaine sécurité et à votre agent

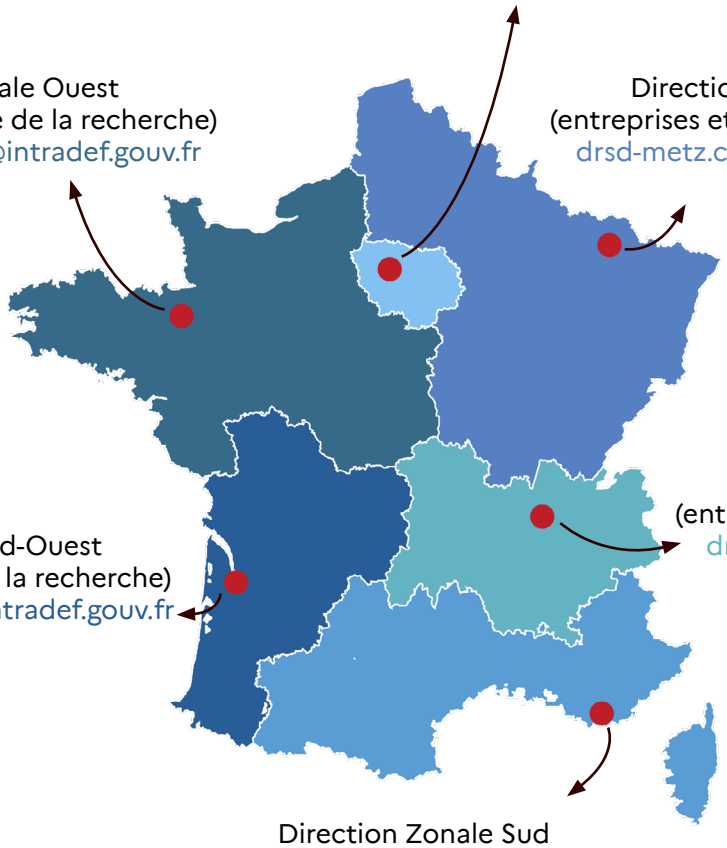
Gardons le contact

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