Lettre d'information économique

Sommaire

Mai 2022

Editorial

Mesdames, Messieurs,

L'activité économique a toujours été corrélée aux turpitudes et déséquilibres du monde : à chaque temps sa combinaison de crises, calque tragique de tensions, de forces et de fragilités appliqué à un tissu politique, économique, humain toujours différent.

Notre ère n'est pas exempte de phénomènes déstabilisants, sources d'incertitude et générateurs de défis à relever.

Au cœur de l'empilement actuel de crises sanitaire, sécuritaire, sociale et désormais guerrière, l'activité économique, industrielle, intellectuelle et expérimentale de défense occupe une place singulière. Sa singularité s'exprime au travers d'une triple particularité.

Tout d'abord, à l'instar de toute activité économique, sa performance est dépendante de la stabilité des sociétés dans lesquelles elle s'inscrit. Par ailleurs elle est aussi directement impliquée dans la crise par sa contribution directe à l'action des États, puisque la logique industrielle de défense la caractérise. Enfin elle est elle-même au cœur de la confrontation économique qui cible l'excellence des savoir-faire du concurrent, et ses capacités.

Cette lettre d'information économique s'adresse aux grands acteurs industriels, à la multitude d'ETI, PME et TPE qui concourent à la puissance de la défense française, aux jeunes sociétés et startups, comme aux unités de recherche qui conçoivent et produisent les succès de demain.

C'est donc pour mieux les protéger que cette lettre offre un éclairage sur les salons d'armement dont la tenue, dans le contexte actuel, prend un relief particulier. Ils sont les miroirs des meilleures capacités industrielles françaises, un concentré éclairant des outils de gestion de crise les plus innovants, mais aussi un tremplin commercial pour la conquête de marchés en pleine extension.

À ce titre, ils attirent les intérêts, intelligences et convoitises de nos compétiteurs étatiques comme infra-étatiques. Les salons étant un lieu privilégié de promotion et de prospection, les sociétés doivent y rayonner, tout en étant préservées. Ainsi, les actions de détection et de protection concernent les exposants sur le site pendant l'événement, mais aussi chaque collaborateur des sociétés dans son environnement élargi, ses outils numériques, ainsi que ses déplacements pendant cette activité.

Détecter ces menaces fait partie des missions de la DRSD : ses agents s'y engagent, sur le territoire national comme à l'étranger, en amont, au cours et en aval des salons. C'est une mission qu'elle assure de conserve avec les acteurs industriels, car il n'est pas question de laisser des intervalles aux compétiteurs contrevenant à la pérennité de notre industrie de défense, aux actifs que l'État investit dans son activité, et de façon ultime à la souveraineté nationale.

Général de Corps d'Armée Eric Bucquet

Directeur du Renseignement et de la Sécurité de la Défense

Bilan 2021 des ingérences
en matière de sécurité économique

I. Recrudescence des menaces dans un contexte post-crise

Exacerbés par la crise sanitaire et économique, les enjeux de souveraineté économique ont ravivé l'implication des Etats dans la protection des sociétés stratégiques. Ainsi, en 2021, sur la base des éléments dont elle a eu connaissance, la DRSD a constaté une **augmentation du nombre d'ingérences** à l'encontre de la base industrielle et technologique de défense (BITD) nationale. Effectivement, le nombre de menaces décelées en 2021 est quasiment remonté à son niveau d'avant la crise du coronavirus, avec environ 700 cas traités.

En 2021, en dépit d'une reprise économique lisible mais inégale et de la persistance des vagues épidémiques, la reprise des salons d'armement et des visites en entreprise ont relancé à la hausse le nombre d'atteintes humaines, particulièrement celles ciblant les collaborateurs à haute technicité ou maîtrisant de rares savoir-faire. Cette ressource humaine qualifiée est d'autant plus convoitée que le contexte économique abrasif a engendré des difficultés de recrutement et de fidélisation.

En matière de cybercriminalité, tous les secteurs d'activité ont été affectés en 2021. Parmi les modes opératoires privilégiés par les cyberattaquants, les attaques par rançongiciel sont restées la principale menace. Par ailleurs, les attaques par hameçonnage se sont maintenues à un niveau élevé. Ces modes opératoires peuvent constituer les vecteurs d'exfiltrations de données sensibles ou d'attaques par rebond vers d'autres entreprises liées à l'entité ciblée. D'autant que l'extension continue de la chaîne de valeur et les interconnexions associées, notamment dans le cyberespace, augmente la surface d'attaque cible des cyberattaquants.

En parallèle, les ingérences fondées sur l'interprétation extensive, voire l'instrumentalisation, du droit et des réglementations à portée extraterritoriale, se sont maintenues en 2021. Dans un contexte de concurrence accrue entre les entreprises sur les marchés à l'export, l'utilisation de ces dispositifs juridiques extraterritoriaux a continué de servir la politique de souveraineté d'Etats compétiteurs en ciblant notamment les secteurs stratégiques.

II. Les secteurs de la défense particulièrement ciblés

En 2021, l'ensemble des secteurs de la base industrielle et technologique de défense (BITD) nationale a continué de susciter un intérêt marqué, notamment de la part des plus grandes nations connues pour leur stratégie offensive (Etats-Unis et Chine, entre autres). À l'instar de 2021, les secteurs les plus ciblés demeurent les technologies de défense et de sécurité, l'aéronautique et le domaine spatial, les technologies de l'information et de la communication, la construction navale, les industries de matériaux, de métallurgie et de chimie.

III. De nouvelles vulnérabilités en perspective

De manière prospective, en 2022, les ingérences pourraient s'étoffer en exploitant des vulnérabilités ou des circonstances de trois ordres : l'exploitation des déficits de conformité aux lois à portée extraterritoriale, le ciblage activiste des difficultés de financement et enfin l'utilisation opportuniste du contexte géopolitique actuel.

Bilan 2021 des ingérences
en matière de sécurité économique

Dans un contexte de guerre économique de plus en plus assumée entre les États-Unis et la Chine, les ingérences liées à l'extraterritorialité devraient augmenter. La Chine a officialisé en 2020 son dispositif juridique lié à l'export, dont l'application risque d'engendrer de nombreuses ingérences au fur et à mesure de sa montée en puissance et de sa mise en œuvre. Cette consolidation juridique chinoise rejoint celle d'autres États dotés de corpus similaires mais ne disposant pas de la même force économique (Royaume-Uni, Brésil notamment). N'étant plus seulement exposées au seul arsenal juridique américain, les sociétés françaises pourraient progressivement faire face à un risque démultiplié d'ingérence par le biais d'ingénieries juridiques ou normatives à portée extraterritoriale.

Sur le plan financier, l'extrême sensibilité en matière de conformité et la prévention du risque des banques sont motivées par le développement d'une interprétation extensive de la responsabilité sociétale des entreprises. À terme, cela est susceptible de fragiliser l'accès aux financements des sociétés de défense, plus particulièrement aux PME/PMI, induisant des vulnérabilités exploitables par des acteurs ingérents par le biais d'actions de rachats ou de manœuvres de destabilisation.

Depuis plus d'un mois, le contexte lié au conflit en Europe de l'Est voit s'imbriquer les concepts d'économie de guerre et de guerre économique. **Les sociétés de la BITD française**, par leur activité sectorielle directement liée aux armées pour les unes, et par leur savoir-faire contributif, ciblé ou dual, pour d'autres, **sont *de facto* positionnées sur un front parallèle à celui des effets politiques et diplomatiques.** Cette autre ligne de confrontation est composée d'effets directement induits (bouleversement des tarifs et des marchés), ou résultant des actions contraignantes des différentes parties (sanctions et contre-sanctions).

Pour en savoir plus sur les risques liés au contexte géopolitique, consultez la LIE FLASH spéciale UKRAINE.

Bilan 2021 des ingérences
dans le domaine cybernétique

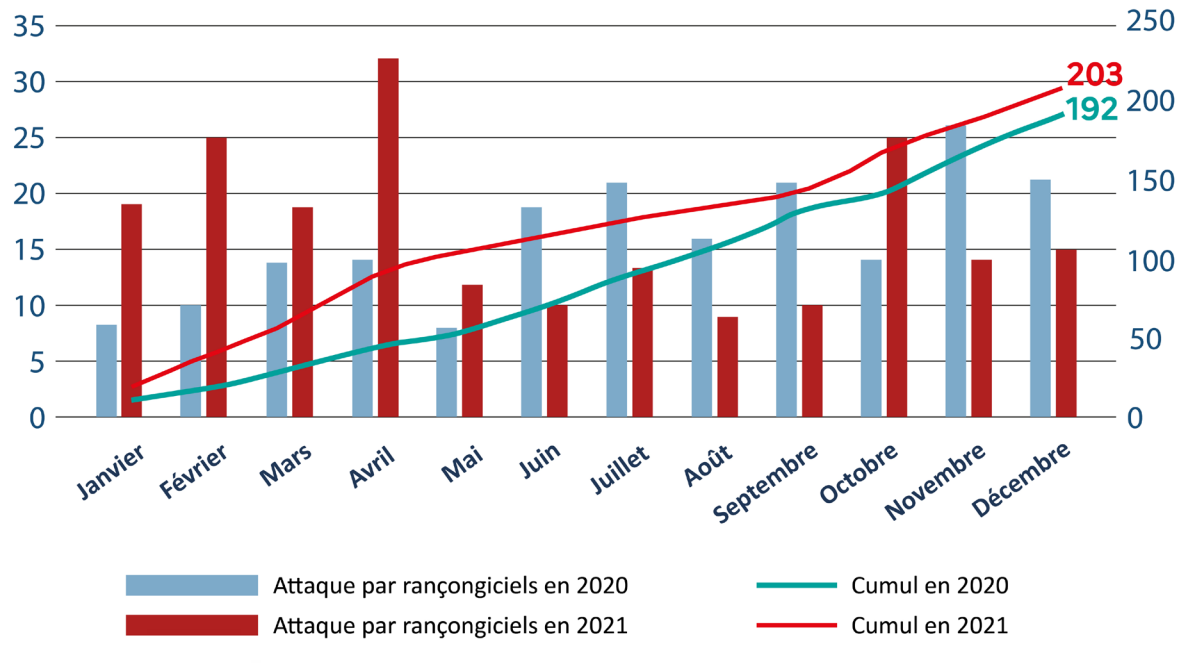
I. La cybercriminalité, une menace avérée et croissante pour la BITD

L'année 2021 a été marquée par une **activité cybercriminelle importante.**

La menace **rançongiciel** continue sa progression sur 2021, en particulier à l'égard des PME, TPE et ETI de l'ensemble des secteurs d'activité de la BTID. En outre, la banalisation du *Ransomware as a Service*[1] (RaaS) illustre et facilite le développement de réseaux criminels organisés. Ce type d'attaque entraîne des **fuites de données sensibles** et provoque un **préjudice élevé pour les entreprises sur les plans financiers, de la production, parfois juridique et même réputationnel.**

Les attaques par **hameçonnage** constituent également un axe puissant d'affaiblissement. En effet, ces attaques peuvent viser des exfiltrations de données sensibles ou la perpétration d'attaques par rebond réorientées vers d'autres entreprises liées à l'entité affectée. À ce titre, la **chaîne d'approvisionnement logistique** de la BITD est une cible d'intérêt pour des acteurs malveillants.

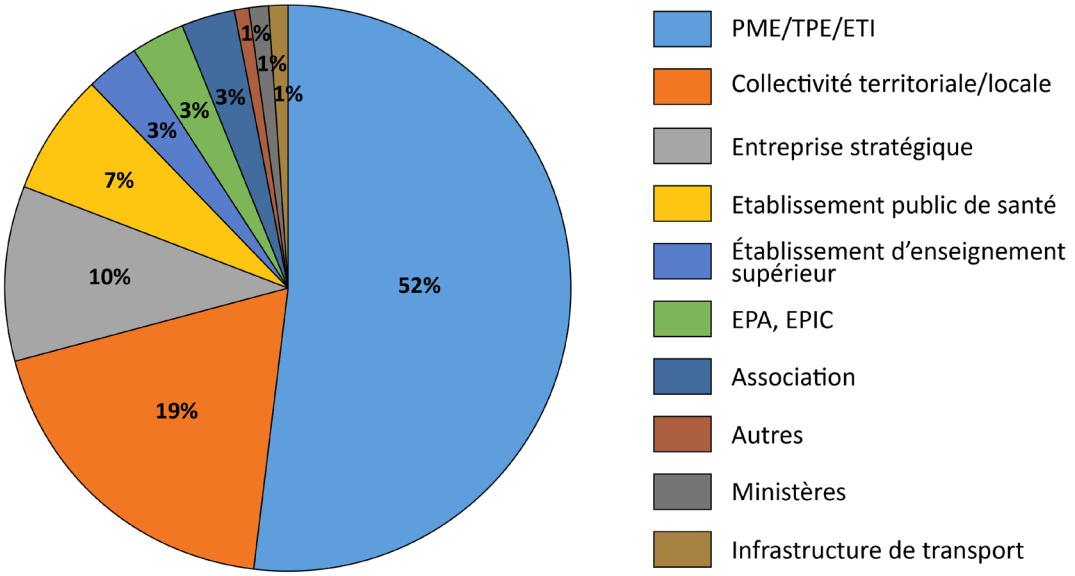
En effet, par ce biais, l'attaquant peut potentiellement mener une attaque par rebond afin d'atteindre de façon détournée un industriel important.



Attaques par rançongiciels traitées par l'ANSSI en 2020 et 2021 tous secteurs d'activités confondus

[1] *Ransomware as a Service* (RaaS) : mise à disposition, clés en mains, par un groupe de cybercriminel, d'un rançongiciel et de son mode d'emploi. Une telle offre permet à des pirates informatiques d'accéder à un maliciel même s'ils n'ont pas les compétences pour les développer.

Répartition des entités victimes d'attaques par rançongiciel



Répartition des entités victimes d'attaques par rançongiciel
dans le cadre des incidents traités par l'ANSSI en 2021

Panorama des menaces et incidents ANSSI 2021 : https://www.cert.ssi.gouv.fr/

II. Le cyberespionnage, une menace latente pour la BITD

En 2021, une série de campagnes malveillantes relevant possiblement du cyber-espionnage a visé la BITD. Des tentatives d'ingérences étrangères ont été observées au cours de l'année, avec des approches commerciales d'institutions et d'entreprises étrangères auprès d'entités de la BITD. Ainsi, les approches par les réseaux sociaux professionnels tel que LINKEDIN restent un mode opératoire pour les acteurs malveillants. De telle actions peuvent être menées, soit dans l'optique d'approcher une personne en vue d'acquérir des informations sur des avancées technologiques, soit pour introduire un maliciel. Les objectifs poursuivis par les cyberattaquants peuvent être l'altération des données (recours massifs aux *wipers* visant à effacer vos données), l'influence mais encore l'espionnage (pour plus d'information, voir la LIE d'octobre 2020).

III. Conclusions

Le Service a observé une **activité cybercriminelle significative à l'encontre de l'ensemble des secteurs** de la BITD en 2021. Pour faire face à cette menace au cours de l'année à venir, le Service poursuivra sa mission d'accompagnement et de conseil auprès des acteurs de la sphère défense lors de la remontée d'information, de constat ou de détection de vulnérabilités majeures. De même, le Service sera attentif aux actes malveillants pouvant relever du cyberespionnage afin de **prévenir la captation de savoirs, de données sensibles et d'exfiltrations liées au potentiel scientifique et technique de la nation (PSTN) pouvant mettre à mal la souveraineté nationale.**

Évolution des modalités d'application de la loi dite " de blocage "

(loi n°68-678 du 26 juillet 1968)

Très récemment, plusieurs dispositions légales (le décret du 18 février 2022 et l'arrêté du 7 mars 2022) ont renforcé le dispositif national de protection économique face à l'accroissement des lois à portée extraterritoriale et de leurs champs d'application.

Objectif : *« Permettre d'éviter que les autorités étrangères ne viennent connaître des informations sensibles attentant aux intérêts de la Nation, y compris ses intérêts économiques essentiels, lors d'enquêtes. Cette évolution vise à obliger les autorités étrangères à respecter les canaux de l'entraide judiciaire ou administrative internationale ».*

Source : Ministère de l'économie, des finances et de la relance.

Modifications principales :

Le **décret du 18 février 2022** instaure deux principaux changements. Tout d'abord, il désigne le Service de l'information stratégique et de la sécurité économiques (SISSE) comme guichet unique pour les acteurs concernés afin de leur offrir un seul et unique interlocuteur.

Ensuite, il vient renforcer la sécurité juridique des entreprises en leur permettant de disposer, si elles le souhaitent, d'un avis de l'administration. Ce dernier s'inscrit dans un calendrier adapté aux procédures administratives et judiciaires et vient ainsi renforcer l'opposabilité de la loi de blocage vis-à-vis des juridictions étrangères.

L'arrêté du 7 mars 2022 procède à une clarification des documents attendus lors de la procédure et instaure **l'obligation** de recourir à des **moyens de transmission sécurisés des données échangées.**

Contact utile pour les entreprises :

loi.deblocage@finances.gouv.fr

POUR ALLER PLUS LOIN

Loi n° 68-678 du 26 juillet 1968 :
https://www.legifrance.gouv.fr/loda/id/JORFTEXT000000501326

Décret n°2022-207 du 18 février 2022 :
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045190519

Arrêté du 07 mars 2022 :
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000045358485

Gauvain, R., ***Rétablir la souveraineté de la France et de l'Europe et protéger nos entreprises des lois et mesures à portée extraterritoriale*****,** Rapport à la demande du Premier Ministre Monsieur Edouard Philippe, Assemblée nationale, juin 2019, 102 p. : https://www.vie-publique.fr/sites/default/files/rapport/pdf/194000532.pdf

MINISTÈRE DE L'ÉCONOMIE DES FINANCES ET DE LA RELANCE
Liberté
Égalité
Fraternité

Nos partenaires de confiance

SISSE
Service de l'Information Stratégique et de la Sécurité Économiques

Les salons de défense : opportunités et risques en matière de sécurité économique

Pour les entreprises de la BITD, les salons d'armement constituent traditionnellement des « **vitrines commerciales** » leur permettant d'entrer concrètement en contact avec des interlocuteurs étrangers, partenaires ou clients.

Pour les plus importants d'entre eux les salons réunissent durant plusieurs jours et dans un espace limité, plusieurs centaines de stands professionnels, accessibles à des visiteurs venus du monde entier.

Bien que faisant l'objet de mesures de sécurité rigoureuses, ces manifestations demeurent propices à des **tentatives d'approches intrusives** et à des **captations d'informations non consenties.**

Il est rappelé que lors d'un salon, les entreprises participantes doivent se montrer particulièrement vigilantes à l'égard des **comportements suspects**, à l'instar des **questions intrusives** concernant les **attributs d'une brique technologique** ou encore à la protection de la vie privée de leurs collaborateurs. Par ailleurs, la forte **affluence** qui peut survenir durant ces évènements peut être **mise à profit** par des **personnes mal intentionnées** pour **procéder à des prises de vues non autorisées**, ou encore à des **vols** de matériel. Aussi, les exposants doivent **maintenir une surveillance constante** de leur stand et **éviter les égarements de supports** (informatiques, papiers, etc.) Cette vigilance doit être maintenue lors des phases de montage et de démontage des stands.

Par ailleurs, les évènements en marge du salon (conférences, « *afterworks* », etc.) ne doivent pas être **sous-estimés** puisqu'ils sont souvent propices à des tentatives de ciblage. Enfin, il convient **d'éviter la tenue de conversations professionnelles dans les transports en commun** et ne pas laisser de **supports sensibles dans les chambres d'hôtel**. S'agissant des **salons à l'étranger**, une attention particulière est demandée aux représentants d'entreprises françaises sur ces modes d'action mais également lors du **passage aux douanes.**

Par conséquent, et conformément à ses prérogatives attribuées en matière de contre-ingérence économique, la DRSD recommande le signalement de tout comportement suspect.

Les salons de défense :
le risque cybernétique

Les salons sont des environnements porteurs d'opportunités commerciales mais aussi de menaces cybernétiques. Les ondes WIFI, employées par l'organisateur et les exposants, constituent une cible à fort intérêt pour un acteur malveillant. Différentes types d'attaques sont envisageables.

De fait, toute communication non chiffrée – donc non protégée – ou chiffrée avec un algorithme faible, tel que WEP, doit être considérée comme potentiellement interceptée.

L'un des modes opératoires des acteurs ingérents est la mise en œuvre de faux points d'accès WIFI. Imitant un point d'accès légitime, ce leurre est le vecteur potentiel de nombreuses actions malveillantes : vol de données sensibles comme des identifiants de connexion, piratage des appareils connectés par injection d'un code malveillant, abaissement du niveau de sécurité des communications chiffrées, etc.

Le WIFI n'est pas l'unique technologie sans fil à surveiller. En effet, le *Bluetooth* et la 5G peuvent également être porteurs de vulnérabilités et de menaces. En particulier, les objets connectés reposant sur ces technologies sont insuffisamment sécurisés et peuvent être facilement piratés.

Les connexions physiques doivent également être l'objet de vigilance. En effet, le branchement de dispositifs de type clés USB à un système d'information peut permettre de conduire des attaques cybernétiques. Ainsi, des « bombes logiques » destinées à endommager le matériel ou des maliciels permettant des actions d'espionnage peuvent être propagés par ce moyen.
La DRSD recommande donc les actions suivantes :

- les SI utilisés durant un salon doivent être exclusivement dédiés à cette tâche ;
- ils doivent contenir le strict minimum d'informations nécessaire au salon afin de réduire la surface d'attaque ;
- ces derniers ne doivent pas être reliés aux réseaux de l'entreprise au retour du salon sans avoir fait, au préalable, l'objet d'une analyse antivirale approfondie ;
- tout document récupéré doit être passé en station blanche antivirale avant son intégration au SI de l'entreprise ;
- avant réutilisation, les équipements utilisés doivent faire l'objet d'un effacement de sécurité intégral.

Les salons de défense :

Évènement clef de la mission de contre-ingérence de la DRSD

Les entreprises de la BITD sont régulièrement exposées à des menaces multiples dont l'espionnage (humain et/ou technique), la subversion, le terrorisme voire la criminalité et la délinquance.
Celles-ci se manifestent également lors des salons d'armement où les entreprises se déplacent pour exposer leurs savoir-faire et leurs technologies innovantes et rencontrer des interlocuteurs très diversifiés.

C'est donc pour aider ces entreprises françaises à contrer ces menaces que le Service, dans le cadre de sa mission de protection du potentiel scientifique et technique de la Nation, est présent lors de ces évènements.

De fait, la DRSD organise, en liaison avec ses partenaires, les opérations de couverture des grands salons internationaux de défense se déroulant sur le territoire national. Elle planifie et coordonne la couverture du salon à EUROSATORY et à EURONAVAL, et les années impaires au salon international de l'aéronautique et de l'espace (SIAE) et à MILIPOL. Ce dernier salon a la particularité d'être sous le patronage du ministère de l'Intérieur contrairement aux trois autres qui demeurent sous celui du ministère des Armées.

L'action du Service ne se limite cependant pas à la durée du salon. En effet, quand l'identité des exposants est connue, une action de sensibilisation est prévue en amont du salon.
Pour d'autres salons, dont la couverture opérationnelle est organisée par les directions zonales, le Service est également présent avec un dispositif moins conséquent. La DRSD remplit également sa mission de sensibilisation et de protection à l'étranger dans le cadre de certains salons.

Ainsi, le poste du renseignement et de la sécurité de la défense (PRSD) d'Abu Dhabi (Emirats arabes unis) est régulièrement engagé lors de la tenue des salons d'armement au Moyen-Orient.
Il y intervient pour sensibiliser les acteurs français de l'industrie de défense aux menaces identifiées et, auxquelles ils peuvent être confrontés et recueille les difficultés qu'ils ont pu rencontrer au cours du salon. Cette action de sensibilisation permet de renforcer la vigilance de tous les intervenants français afin de déceler, dans le flot de rencontres, des comportements suspects.
Pour cela, le PRSD local rencontre, en amont, les industriels présents sur le territoire afin de mieux connaître leur engagement pour le salon et mieux déceler les éventuelles vulnérabilités. Ce dernier point est particulièrement important pour les entreprises jeunes, à l'origine de technologies prometteuses, mais parfois peu conscientes de l'intérêt que leur savoir-faire peut susciter.

La présence du PRSD lors des salons, au plus près des intérêts français, permet également de détecter au plus vite des comportements suspects, contribuant ainsi pleinement à sa mission de contre-ingérence. Cette action est réalisée en lien étroit avec les industriels qui sont des maillons indispensables de la chaîne de sécurité et d'alerte.

Les informations capitalisées puis exploitées lors de chaque action, puis exploitées, permettent de faire progresser la sécurité de tout l'écosystème français en ajustant au vue des acteurs ingérents et de leurs modes d'action la sensibilisation dispensée auprès des industriels lors des salons suivants.

Ainsi, lors du prochain salon EUROSATORY, prévu du 13 au 17 juin 2022 à Paris-Nord Villepinte, le Service sera de nouveau présent aux côtés des industriels de la défense. Il y sera joignable via un numéro vert : 01 46 73 56 65 / 06 33 71 01 07.

Les bonnes pratiques :
Lors des déplacements professionnels

Vos collaborateurs ou vous-même effectuez régulièrement des déplacements professionnels. Cette sélection de recommandations concrètes et opérationnelles devrait vous intéresser.

Avant le déplacement

Numérique

- ☑ N'emportez pas de données superflues (ordinateur et téléphone vierges)
- ☑ Sauvegardez les données que vous transportez
- ☑ Protégez l'accès de vos appareils et applications par des mots de passe robustes
- ☑ Privilégiez l'envoi numérique et la récupération de fichiers chiffrés sur votre lieu de mission

Information

- ☑ Informez-vous sur la législation du pays de déplacement (chiffrement, usages)
- ☑ Inscrivez-vous sur le fil Ariane du Ministère de l'Europe et des Affaires Étrangères
- ☑ Préparez votre passage en douane
- ☑ Entretenez-vous avec votre chaîne de sécurité et votre agent DRSD

Pendant le déplacement

En permanence

- ☑ Faites preuve de discrétion (filtres de confidentialité, discussion dans les lieux publics et privés)
- ☑ Maintenez une vigilance en présence de tiers (bar, taxi, restaurant, etc.)
- ☑ Soyez prudent vis-à-vis des cadeaux (risque de corruption, ou piégeage de clés USB, etc.)
- ☑ Ne laissez pas de données sensibles dans les coffres d'hôtels ou dans les chambres. Emportez vos appareils en permanence avec vous
- ☑ Informez votre chaîne de sécurité et RSSI en cas de vol, perte ou confiscation

Pendant le salon

- ☑ Soyez constamment vigilant, prévoyez un gardiennage
- ☑ Apportez un broyeur sur le salon, une armoire forte
- ☑ Ne laissez jamais le stand et les matériels sans surveillance
- ☑ Observez les comportements des personnes autour du stand
- ☑ Conservez toute information sensible sur vous
- ☑ Surveillez les délégations étrangères
- ☑ Méfiez - vous des repas offerts et pouvant donner lieu à des excès.

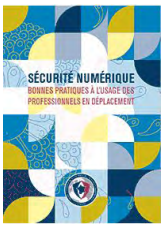
Après le déplacement

Nettoyage

- ☑ Effacez l'historique des appels, de la navigation et des messages de vos appareils
- ☑ Changez les mots de passe utilisés durant le déplacement
- ☑ Faites analyser vos appareils / incentives informatiques par la SSI de votre entreprise
- ☑ Informez votre chaîne de sécurité et RSSI en cas de vol, perte ou confiscation

RETEX

- ☑ Faites un bilan concerté avec l'ensemble des participants
- ☑ Partagez ce bilan avec votre chaîne de sécurité ainsi qu'avec votre correspondant DRSD
- ☑ Avoir le « bon » réflexe : En cas de doute : n'hésitez pas à nous contacter



Nos partenaires de confiance

Gardons contact

Directions Zonales Ile-de-France :
Entreprises : **drsd-dsezp.cmi.fct@intradef.gouv.fr**
Instituts et écoles de recherche : **drsd-idf.cmi.fct@intradef.gouv.fr**

Direction Centrale de contre-ingérence économique : section Sensibilisation
drsd-cie-sensibilisation.contact.fct@intradef.gouv.fr

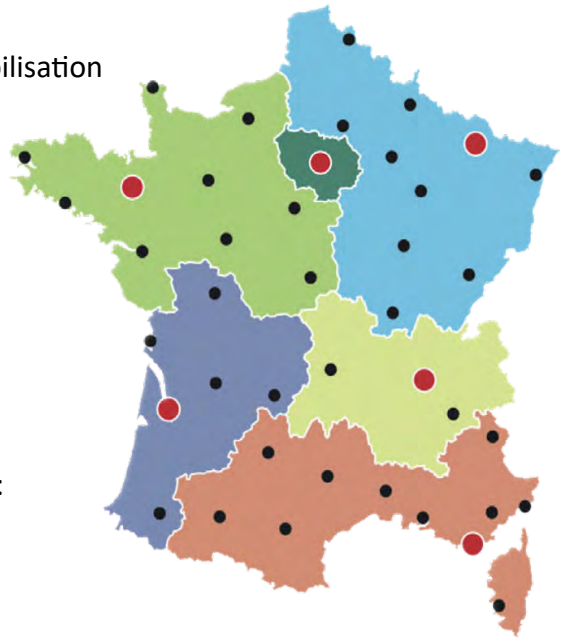
Direction Zonale Nord-Est (entreprises et monde de la recherche) :
drsd-metz.cmi.fct@intradef.gouv.fr

Direction Zonale Ouest (entreprises et monde la recherche) :
drsd-rennes.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



Restons en contact