Lettre d'information économique

Spéciale EURONAVAL 2022

LE SALON MONDIAL DU SECTEUR NAVAL DE LA DÉFENSE

Septembre 2022

Editorial

Mesdames, Messieurs,

Le salon EURONAVAL 2022 se déroulera, du 18 au 21 octobre 2022, au parc des expositions du Bourget (93). Cette 28e édition est d'autant plus attendue que la 27e (2020) n'avait pu se dérouler qu'en format digital du fait de la crise sanitaire.

Moment privilégié d'opportunités d'affaires et de visibilité pour votre entreprise auprès des principaux décideurs économiques ainsi que des états-majors, cet évènement représente également pour certains acteurs étrangers, publics comme privés, une opportunité de conduire des actions d'ingérence de toutes natures et pouvant porter atteinte aux intérêts économiques et réputationnels de votre entreprise, voire de vos collaborateurs et de vos partenaires.

Conformément à ses missions de contre-ingérence et de protection de l'intégrité du secret de la défense nationale au contact de tous les industriels de défense, et tout particulièrement dans un contexte géopolitique sous haute tension marqué par les confrontation économiques et géopolitiques accrues du conflit entre la Russie et l'Ukraine, les agents de la Direction du Renseignement et de la Sécurité de la Défense (DRSD) seront à vos côtés durant toutes les étapes du salon.

Vous trouverez ci-après les principales recommandations en matière de protection physique et cybernétique à mettre en place avant, pendant et après votre participation au salon. Nous vous invitons à les diffuser largement à vos collaborateurs, prioritairement ceux engagés sur le salon.

N'hésitez pas à contacter votre agent référent DRSD afin de faire remonter toute ingérence ou atteinte (physique, économique, juridique, cybernétique, etc.) dont vous penseriez être victimes et / ou témoins.

En cas de difficulté, il vous sera possible de joindre **notre équipe sur place** via les numéros :

01 46 73 56 65 / 06 33 71 01 07

La sécurité et la sûreté de la base industrielle et technologique de défense nationale (BITD) repose sur la sensibilisation, la prise en compte et l'anticipation des enjeux par tous ses acteurs.

Afin de vous permettre d'aborder ce salon international dans les meilleures conditions, je vous assure de l'engagement total des agents de la DRSD à vos côtés dans ce contexte aussi singulier que versatile.

Je vous souhaite un excellent salon EURONAVAL 2022.

Général de Corps d'Armée Eric Bucquet

Directeur du Renseignement et de la Sécurité de la Défense

PRINCIPAUX RISQUES

- Terrorisme / sabotage ;
- Espionnage (ex. vols de procédés de fabrication, d'innovation ; de prospects et contrats commerciaux, etc.) ;
- Débauchage / chantage ;
- Cyber (ex. intrusions sur les SI, rançongiciel de données insérées dans un cloud privé & public, etc.).

PRINCIPAUX IMPACTS

- Perte de confiance de vos clients, fournisseurs et autres partenaires ;
- Perte d'avances technologiques ;
- Perte de capacité d'innovation ;
- Perte de marchés, d'avantages concurrentiels.

Volonté affirmée et soutenue de captation de savoir-faire de pointe par certains Etats étrangers et concurrents → **Conséquences systémiques pour votre entreprise et pour la BITD nationale**

PRINCIPAUX MODES OPÉRATOIRES CONSTATÉS

- **Moyens techniques :** tentatives d'implantation de dispositifs discrets d'écoute / de prise de vue / d'interception / d'intrusion ; tentatives de récupération d'échantillon / de prêt / d'achat unitaire ; etc. ;

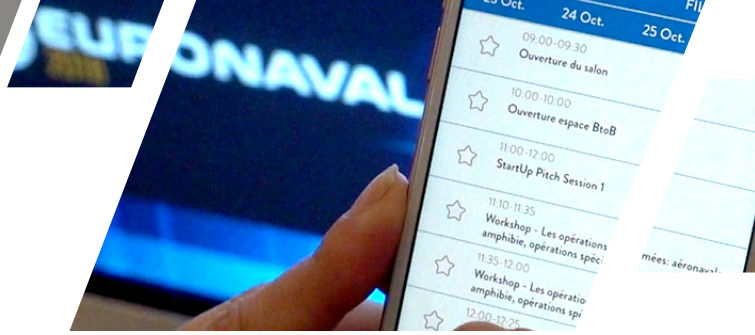
- **Vol de matériels, de supports informatiques et de badges d'exposant** dans les stands, les véhicules / navettes, les hôtels, les restaurants, etc. ;

- **Approche humaine :** détection de contacts utiles par des approches comme la prise d'attache par un « ancien élève ou collaborateur » (notamment via les réseaux sociaux) ; compromission ; cupidité ; crédulité ; demande d'information techniques et capacitaires très intrusives mettant en avant la nécessité de ces données pour un éventuel contrat, etc. ;

- **Cyber :** usurpation de point d'accès réseaux, détournement du wifi, attaque par supports amovibles, phishing, etc. ;

- **Contournement d'embargo / de règlementation.**

Recommandations particulières



3 questions clés à se poser :

1. Quels sont les risques pesant sur ma participation au salon (ex. captation de savoir-faire, tentative de débauchage d'un expert-collaborateur, etc.) ?
2. Quel est mon degré d'exposition à ces risques ?
3. Comment maîtriser ces risques pour les rendre acceptables ?

AVANT LE SALON

La phase d'**ouverture aux professionnels** est la période la plus à risque en matière de protection de matériels, de mouvements et de tentatives d'approche ou de captation.

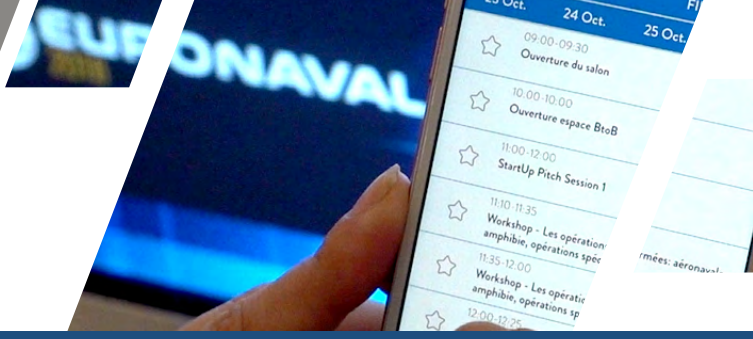
Étudier et évaluer la menace en préparant **en amont** votre exposition

- ☐ **Identifiez les exposants / concurrents / sous-traitants / délégations officielles ainsi que les journalistes** susceptibles de **venir visiter votre stand : préparer un argumentaire spécifique** (*kit de presse, carte de visite*). Notamment sur les **sujets sensibles** (*innovations, business plan, etc.*) ;
- ☐ Effectuez une **veille concurrentielle** pour **évaluer le positionnement de vos concurrents** ainsi que sur les **attendus du salon communiqués par les délégations officielles** ;
- ☐ **Renseignez-vous sur les prestataires de service avec qui vous souhaiteriez collaborer** (*ex. aménagement du stand, personnel d'accueil, etc.*) ;
- ☐ Faites réaliser des **maquettes simples et brevetées** ;
- ☐ Mettez en place un **dispositif de sécurité en dehors des heures d'ouverture** ;
- ☐ **Sensibilisez et responsabilisez** (*réunion de calage pré-salon*), les personnes présentes sur le stand (*responsable du stand, communication, commerciaux, stagiaires, etc.*) sur les risques encourus. **Insister sur l'importance de la maîtrise des enjeux de sécurité et de sûreté en indiquant le POC en cas d'incident** ;
- ☐ **Informez-vous sur les règles en vigueur et de conformité** (*manuel de l'exposant, possibilités et restrictions liées à l'événement, etc.*) ;
- ☐ Consultez le bilan – **retex des salons précédents.**

Étudier l'environnement

- ☐ Répartissez et communiquez les rôles, les jours de présence et les contacts des **acteurs** (*collaborateurs de l'entreprise, stagiaires, prestataires externes, etc.*) ;
- ☐ Étudiez la disposition du salon, **identifiez les sociétés des stands voisins** et **identifiez les visites des délégations étrangères** ;
- ☐ **Ne laissez jamais seul les prestataires de service** (*ex. transports de vos matériels, sur le salon*). **Notamment lors de l'installation du stand** (*décoration, électricité, internet, etc.*) ;
- ☐ **Inventoriez le matériel et les fournitures** qui seront installés sur le stand ;
- ☐ **Limitez la mise à disposition de documentation** (*apporter un broyeur, une armoire forte, une station blanche si nécessaire*) ;
- ☐ Prévoyez un **espace de confidentialité** (*si nécessaire*).

Recommandations particulières



DURANT LE SALON

MAINTENIR UNE VIGILANCE ACCRUE EN MAÎTRISANT VOTRE EXPOSITION

- ☐ **Matin** et **soir**, « **briefez / débriefez** » l'équipe sur la sécurité et **faites remonter toutes informations ou doutes** à la chaîne « sécurité / sûreté » de l'organisation ainsi qu'à la DRSD ;
- ☐ Faites preuve d'une **prudence** et d'une **discrétion** constantes et **conservez toute information délicate sur vous ou dans une armoire forte** ;
- ☐ **Ne laissez jamais le stand et le matériel sans surveillance** ;
- ☐ Indiquez clairement **l'interdiction de prise de vues** (*photos, vidéos*) ou de captation audio ;
- ☐ Surveillez les **comportements des personnes** (*notamment des délégations étrangères, ainsi que de leur accompagnant - traducteur*) ;
- ☐ **Assurez-vous systématiquement de l'identité des visiteurs en demandant une carte de visite** (*inscrire le jour, l'heure, le contact interne ainsi que toutes d'informations jugées utiles*) ;
- ☐ **Surveillez** et **emportez le soir** vos matériels sensibles pour éviter les vols et les dégradations ;
- ☐ **Évitez de répondre aux sondages et enquêtes multiples.**

HORS SALON

REDOUBLEZ DE VIGILANCE

Les évènements et les périodes entourant le salon sont propices à la captation d'informations et aux tentatives d'approche.

Déplacements : dès votre arrivée vous pouvez être ciblés / surveillés

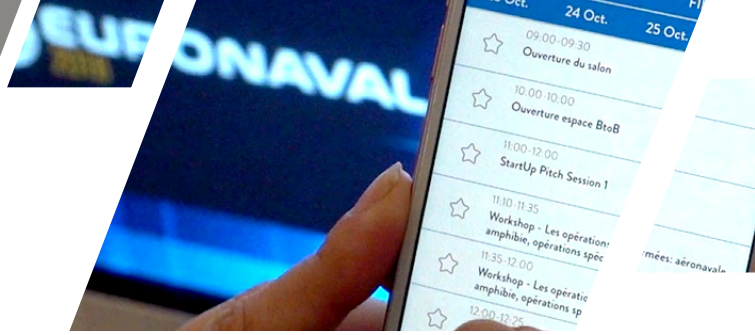
- ☐ Aéroport, gare, parkings : lieux propices au vol de matériel, tentative d'approche humaine, etc. ;
- ☐ Attention à la visibilité de votre badge et à l'écoute de vos discussions dans les lieux publics et transports (*notamment les navettes et les taxis*) ;
- ☐ Apportez une surveillance constante et une mise en sécurité des informations sensibles transportées (*documents, ordinateur, etc.*) ;
- ☐ **Méfiez-vous des rencontres « amicales spontanées »** ;
- ☐ **Évitez d'utiliser les moyens de communication des hôtels, restaurants, gares, aéroports etc. en privilégiant le réseau de votre opérateur** ;
- ☐ **Utilisez des outils spécifiquement préparés et dédiés pour le salon.**

Séjour

- ☐ Votre **chambre d'hôtel n'est pas un lieu sécurisé** (*vol classique…*) : gardez toujours les informations sensibles avec vous ;
- ☐ Soyez **vigilant lors des invitations à des repas, « after-salon »** planifiés **et « non planifiés »** ainsi que des invitations à des conférences tous frais payés / cadeaux (*risque de corruption, ou piégeage de clés USB, etc.*).

Au moindre doute : contacter votre chaîne de sécurité, les organisateurs ainsi que la DRSD

Recommandations particulières



LORS DE LA CLÔTURE

« FAITES PLACE NETTE » À VOTRE STAND ET VOS SUPPORTS SI

En fin de salon, fatigue et routine aidant, le niveau de sécurité baisse et les **actions de captation élémentaire** sont fréquentes et s'appuient souvent sur des repérages réalisés en amont.

- ☐ **Assurez-vous de la présence effective** des personnels alloués, dont la société de transport ;
- ☐ **Soyez présent lors du démontage du stand** ;
- ☐ **Réalisez un état des lieux de sortie** avec votre équipe et avec le prestataire de service.

Attention à la période sensible entre le départ des exposants et l'arrivée des prestataires chargés de l'emport du matériel

APRÈS LE SALON

ÉTABLIR ET PARTAGER VOTRE BILAN - RETEX

- ☐ Rédigez un RETEX suite à **une réunion « post-salon »** avec les participants (*impressions, problèmes rencontrés, points d'étonnement, axes d'améliorations, etc.*) en séparant le point « sécurité et sûreté » du point « commercial et attendus » ;
- ☐ **Cyber :**
  - ☐ **Effacer l'historique des appels, de la navigation et des messages de vos appareils** ;
  - ☐ **Changez les mots de passe** utilisés durant le salon ;
  - ☐ **Faites analyser vos appareils informatiques** par la SSI de votre entreprise.

Partagez votre bilan « sécurité / sûreté » avec votre interlocuteur DRSD en toute confiance et confidentialité

- **Utilisez des supports et des systèmes exclusivement dédiés au salon, non connectés à ceux de l'entreprise** et dotés **d'antivirus.** N'y stockez que les **données strictement nécessaires** ;

- **Contrôlez systématiquement vos supports amovibles en station blanche,** notamment si vous transférez des fichiers obtenus sur une plateforme digitale vers le SI de votre société. Un acteur malveillant pourrait chercher à déposer sur la plateforme un rançongiciel qui, une fois téléchargé, serait susceptible de contaminer votre SI ainsi que ceux de vos partenaires ;

- Soyez particulièrement prudent en cas **d'indisponibilité temporaire ou de saturation des connexions** quant à l'utilisation d'autres solutions moins sécurisées et donc plus vulnérables ;

- Soyez **vigilants** face aux risques associés aux **échanges non sécurisés via des plateformes de discussion virtuelle** (*documents ou liens susceptibles de contenir des codes malveillants*) ;

- Isolez-vous dans un **lieu calme** présentant un **fond neutre** ;

- **Coupez systématiquement votre micro en dehors des prises de parole** ;

- **Assurez-vous,** dans la mesure du possible, **de l'identité des participants, y compris hors du champ visuel de la caméra** ;

- **Pensez à vous déconnecter systématiquement en fin de session** ;

- Si vous souhaitez **échanger avec un partenaire spécifique un document** à caractère potentiellement sensible : faites-le via une adresse mail professionnelle ;

- Si possible, **chiffrez vos données à l'aide d'un logiciel reconnu ou labélisé par l'ANSSI.** Les documents chiffrés ne pouvant être scannés par un antivirus, il sera indispensable de les faire analyser après déchiffrement, sans les avoir ouverts ou déplacés. Assurez-vous de la non-divulgation des clefs de chiffrement utilisées au cours du salon afin d'éviter toute compromission lors d'échanges et de négociations avec des clients actuels et potentiels.

SI VOUS CONSTATEZ :

- Comportements étranges et / ou suspects,
- Questionnements intrusifs (notamment lors des évènements hors salon),
- Prises de photographies précises et / ou intempestives,
- Vol (matériels, documentations, objets, etc.),
- Ajout d'un composant cyber (ex. clé USB) :

notez le maximum d'informations et de précisions sur le/les individus et leurs agissements afin de les communiquer à votre chaîne sécurité, aux organisateurs et votre référent DRSD !

POC DRSD au salon : 01 46 73 56 65 / 06 33 71 01 07

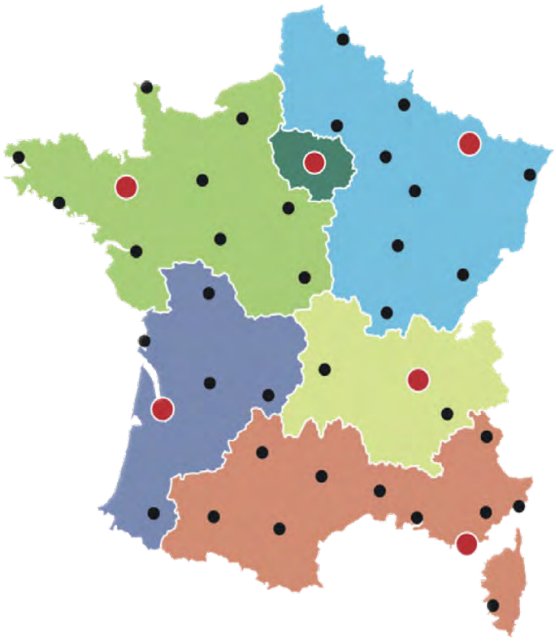
ANSSI

SISSE

Gardons contact

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

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 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