# Lettre d'information économique

## Sommaire



*Mars 2020*

# Editorial

La guerre économique est « une guerre permanente, sans mort apparemment et pourtant une guerre à mort ». Ces mots prononcés par un ancien chef de l'Etat, il y a une trentaine d'années, conservent tout leur sens.

De fait, la DRSD, qui fait partie du dispositif de protection contre les prédations et autres ingérences étrangères, consacre une part croissante de ses capacités à lutter contre ces menaces qui touchent les entreprises en lien avec la Défense.

Un des volets de sa mission, à travers notamment ses actions de sensibilisation dont fait partie cette lettre d'information, consiste à rappeler régulièrement aux entreprises les risques qu'elles encourent et qui évoluent constamment.

Dans le dispositif global de protection, la nouvelle IGI 1300, instruction interministérielle et socle réglementaire qui régit la protection du secret, est en profonde transformation. En cours de réécriture, sa mise en application est prévue à l'été 2021.

Le risque cyber est incontestablement la menace montante qui, rapporté à son coût, occasionne potentiellement le plus de dégâts. La chaîne de sous-traitance apparaissant aujourd'hui comme le point d'attaque privilégié, la consolidation de la cybersécurité de cette *supply chain* devient un enjeu crucial.

Enfin, acteur central de la sûreté en entreprise de défense, l'officier de sécurité doit être considéré comme une "assurance compétitivité" et comme un acteur incontournable de la croissance de l'entreprise, œuvrant au quotidien à éviter des pertes fatales.

Dans cette guerre économique latente, la DRSD, par ses actions de contre-ingérence, contribue directement à la protection des acteurs économiques de la sphère Défense. Grâce à son maillage territorial dense, elle appuie au plus près ces entreprises qui ne doivent pas hésiter à la contacter.

**Général de Corps d'Armée Eric Bucquet**
**Directeur du Renseignement et de la Sécurité de la Défense**

# Ingérences économiques

## Rétrospective 2019

### Un contexte volatile et offensif

Entre concurrence sauvage, tentative de déstabilisation, quête de puissance, rivalités géopolitiques et leurs conséquences économiques, l'année 2019 confirme les tendances déjà observées depuis quelques temps en matière de contre-ingérence économique.

Cette année a été marquée par une remontée d'information vers la DRSD concernant les ingérences économiques ciblant les ETI, PME, PMI ou TPE de la sphère défense, ces dernières ayant pris davantage conscience des enjeux liés à leurs vulnérabilités et aux menaces pesant sur leurs activités. En effet, souvent en quête de capitaux et cherchant à développer leurs activités tant en France qu'à l'international, ces entreprises sont aussi moins préparées pour affronter des actes hostiles ou des ingérences étrangères aux conséquences économiques, financières ou juridiques qui pourraient s'avérer désastreuses. Elles deviennent de fait des cibles de choix ainsi que des vecteurs d'entrées susceptibles de porter atteinte à l'ensemble de l'écosystème.

### Des acteurs décomplexés

Les nations les plus ingérentes, fréquemment citées dans de nombreux médias (Chine, Etats-Unis, Russie…), ne sont pas les seules à représenter une réelle menace. L'année 2019 confirme, en ce sens, une tendance déjà pressentie : plus d'une cinquantaine de nationalités (acteurs étatiques ou privés) est à l'origine des ingérences signalées chaque année. Ces nations, certes plus discrètes, sont elles aussi à la recherche d'information, de connaissances ou de savoir-faire de l'industrie de défense française.

### Tous les secteurs sont touchés

La France se place au 6ème rang économique mondial en matière d'exposition et au 2ème rang européen, en raison de ses secteurs d'activités de pointe, symboles du rayonnement de la France à l'étranger et sources de nombreuses convoitises.

L'aéronautique, le naval ou le spatial, qui concentrent des technologies sensibles et duales à forts enjeux, sont très exposés. Les secteurs de l'information et de la communication, l'intelligence artificielle, les drones sont particulièrement touchés. Enfin, les instituts et laboratoires de recherche qui concentrent des savoirs et savoir-faire de haute technologie suscitent également la convoitise.

### Des modes d'action variés

Aussi variés que les acteurs sont nombreux, les modes d'action exploitent le paradoxe auquel sont notamment confrontées les entreprises françaises de la sphère défense : entre impératif de protection des informations et volonté de bénéficier de la mondialisation. En effet, tout l'enjeu pour ces entreprises est de trouver un équilibre entre la protection de leurs savoirs souverains et les velléités de coopération, de promotion et d'expansion de leurs activités à l'international.

.../...

# Ingérences économiques

Parmi les principaux modes d'action constatés, on retrouve l'utilisation des fragilités et vulnérabilités humaines notamment par le biais des réseaux sociaux, les sollicitations pour de faux entretiens d'embauche ou des cas de débauchages. Autres pratiques répandues : les invitations à participer à des conférences à l'étranger, ou encore des propositions de collaboration avec des Etats sur la base d'un socle idéologique, religieux ou culturel commun.

Le recours aux attaques cyber protéiformes et ciblées afin de récupérer des informations stratégiques ou sensibles est également courant, via le *phishing,* l'ingénierie sociale ou encore le rançonnage. Quant au vol de matériels numériques dans les transports ou dans les hôtels, il reste encore malheureusement trop fréquent.

On observe également un nombre important "d'intrusions consenties" au sein d'entreprises de défense par la voie de visites de délégations étrangères, qui donnent bien parfois des cas avérés de prédations.

Enfin, les promesses d'investissements, la prise de parts capitalistiques par des actifs étrangers, d'une part, les lois extra-territoriales, générant des procédures et des audits de conformité d'autre part, sont autant de modes opératoires aux impacts financiers et juridiques considérables.

## Perspectives et solutions

Les grandes tendances observées ces dernières années, notamment le nombre croissant d'acteurs ingérents, le renforcement des menaces dans les secteurs de pointe et des modes d'action toujours plus élaborés, semblent appelées à perdurer.

Ces ingérences d'ordre économique, souvent mal identifiées ou mal évaluées, peuvent avoir des conséquences commerciales, financières ou juridiques pour la sérénité d'une société. Dans ce contexte, il est important que les entreprises ou organisations renforcent leur "culture sûreté-sécurité" et mettent en œuvre un processus de management des risques global et systémique. Ces mesures permettent d'adopter une posture d'anticipation, de réduire les impacts et d'améliorer la prise de décision.

Les dispositifs techniques et organisationnels pris doivent respecter les textes, lois et règlements en vigueur en matière de :

- sécurisation physique ;
- sécurisation des systèmes d'information, avec des mesures technico-organisationnelles adaptées aux modes opératoires ;
- protection des informations et supports classifiés ainsi que du potentiel scientifique et technique de la nation contre les fuites d'information et les compromissions ;
- conformité et respect des normes nationales et internationales.

Les ingérences économiques, protéiformes et endémiques, continueront toujours de sévir dans des secteurs aussi stratégiques que hautement innovants. Aussi, la mise en œuvre d'une véritable stratégie active de prévention et de protection constitue la mesure la plus efficace pour protéger le patrimoine matériel et immatériel des entreprises et organisations de la sphère défense.

Dans le cadre de sa mission de contre-ingérence économique, la DRSD est particulièrement présente aux côtés des entreprises pour les conseiller et les accompagner dans la mise en œuvre de cette stratégie. ■

[1]*Notamment : IGI 1300, IM 900*

# IGI 1300


## La réforme de la protection du secret de la défense nationale

La réglementation relative à la protection du secret de la défense nationale fait l'objet d'une profonde transformation. Cet article présente les grandes lignes de cette évolution et son calendrier.

### Un nouveau système de classification à deux niveaux

Le décret du 2 décembre 2019 a posé la première pierre de cette transformation en instituant une nouvelle nomenclature de classification. Les articles R2311-2- et R 2311-3 du code de la défense disposent que, à compter du 1er juillet 2021, il existera deux niveaux de classification, utilisés en fonction du degré de sensibilité des données considérées : le niveau Secret et le niveau Très Secret. Chacun de ces niveaux accorde une protection proportionnée au risque encouru en cas de divulgation des informations et supports classifiés (ISC) qu'ils couvrent :

- le niveau Secret protège les informations et supports dont la divulgation, ou auxquels l'accès, est de nature à porter atteinte à la défense et à la sécurité nationale ;
- le niveau Très Secret concerne ceux dont la divulgation aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. Une "classification spéciale" peut être ajoutée au niveau Très Secret. Mais il ne s'agit pas d'un troisième niveau de classification.

.../...

**Le tableau de correspondance entre l'ancienne et la nouvelle classification est établi comme suit.**

| Niveaux (actuels) | Définitions | Niveaux (futurs) | Définitions |
|---|---|---|---|
| **Confidentiel Défense** | ISC dont la divulgation est de nature à nuire à la défense nationale ou pourrait conduire à la découverte d'un secret classifié au niveau Secret Défense ou Très Secret Défense. | **Secret** | ISC dont la divulgation ou auxquels l'accès est de nature à porter atteinte à la défense et à la sécurité nationale. |
| **Secret Défense** | ISC dont la divulgation est de nature à nuire gravement à la défense nationale. | **Très Secret** | ISC dont la divulgation ou auxquels l'accès aurait des conséquences exceptionnellement graves pour la défense et la sécurité nationale. |
| **Très Secret Défense** | ISC qui concernent les priorités gouvernementales en matière de défense et de sécurité nationale et dont la divulgation est de nature à nuire très gravement à la défense nationale. | **Très Secret classification spéciale** | Concerne les ISC de niveau TS faisant l'objet d'une classification spéciale relatifs à des priorités gouvernementales en matière de défense et de sécurité nationale. |

# IGI 1300

## Une nouvelle IGI 1300 en cours de rédaction

La mise en œuvre de la nouvelle nomenclature suppose la refonte d'une instruction générale interministérielle dite « IGI 1300 ». C'est ce texte qui fixe les conditions d'accès des personnes physiques et morales au secret de la défense nationale et établit les règles leur permettant de produire et détenir des ISC ainsi que d'en garantir la protection contre tout risque de divulgation non autorisée.

La version actuellement en vigueur date de 2011. Elle est donc en cours de modification afin de tenir compte de la nouvelle nomenclature. Par ailleurs, le SGDSN, qui tient la plume, travaille en concertation avec l'ensemble des ministères pour procéder à une restructuration et à une actualisation du texte.
La DRSD est associée au travail. La nouvelle IGI 1300 sera plus claire et plus simple à utiliser. Deux points méritent d'être mentionnés :

- le rôle de l'officier de sécurité est détaillé avec plus de précision que dans l'IGI 1300 actuelle, notamment en ce qui concerne sa désignation, ses missions ainsi que sa collaboration avec l'OSSI ;
- globalement, la nouvelle IGI 1300 vise à rendre plus rigoureuses les règles de classification, afin d'éviter la surclassification tout en renforçant la protection des documents classifiés.

## Calendrier prévisionnel

Le texte de l'IGI a été transmis à tous les ministères, qui ont fait part de leurs remarques au SGDSN mi-février 2020. Après cette phase de consultation interministérielle, le texte sera validé et devrait être publié à l'été 2020.

Parallèlement, la DRSD travaille, en lien étroit avec la DPID*, à la rédaction de l'instruction ministérielle dite « IM 900 », qui décline l'IGI 1300 pour le Ministère des Armées et qui devrait elle aussi être publiée à l'été 2020.

Ainsi, les textes finalisés de l'IGI 1300 et de l'IM 900 sont attendus pour l'été mais n'entreront en vigueur qu'un an après. Cette période de transition laissera une année aux acteurs de la protection du secret de la défense nationale pour prendre connaissance des nouvelles règles et des consignes d'accompagnement, afin de les mettre pleinement en œuvre à compter du 1er juillet 2021.

La DRSD vous accompagne au cours de la période de transition pour vous aider à appréhender les nouvelles législations. ■

**DPID : Direction de la protection des installations, moyens et activités de la Défense*

# Supply Chain

## La cybersécurité un enjeu pour la sous-traitance

Ainsi que le soulignait Madame Florence Parly, Ministre des Armées, lors du forum international de la cybercriminalité de 2019, « *plus les Armées se protègent, plus les industriels, les sous-traitants sont susceptibles d'être des proies toutes désignées pour pénétrer dans nos systèmes d'information. Alors, c'est toute la chaîne de Défense qui doit être protégée de bout en bout.* »

La cybersécurité est en effet devenue en quelques années un enjeu vital pour la chaîne de sous-traitance, exposée à des menaces toujours plus sophistiquées, susceptibles de porter atteinte à la disponibilité des systèmes d'information ou à la confidentialité des projets. Si des tentatives d'attaques cybercriminelles de type ransomware sont régulièrement observées, des cyberattaques dites "par rebond" sont également susceptibles d'être menées contre la *supply chain*. Les pirates espèrent ainsi *in fine* atteindre les principaux donneurs d'ordre.

### Attaques "par rebond"

Dans ce cas, les groupes d'attaquants cherchent dans un premier temps à identifier les prestataires de service possédant un lien numérique (canal VPN,..) avec un industriel ciblé. Ces prestataires sont alors victimes d'attaques ayant pour but d'obtenir des droits privilégiés sur leurs réseaux, permettant ensuite d'emprunter les liens numériques établis vers l'industriel visé, au moyen de comptes considérés comme légitimes par ce dernier.

La tendance accrue de recourir à l'externalisation de la maintenance des éléments de l'infrastructure réseau accroît significativement ce type de risque si la cyberprotection n'est pas parfaitement assurée par les entreprises tierces. Par rebond, ce sont en effet potentiellement plusieurs industriels, en recourant aux mêmes prestataires de service, qui peuvent être touchés par une attaque réussie.

### Des capacités techniques complexes

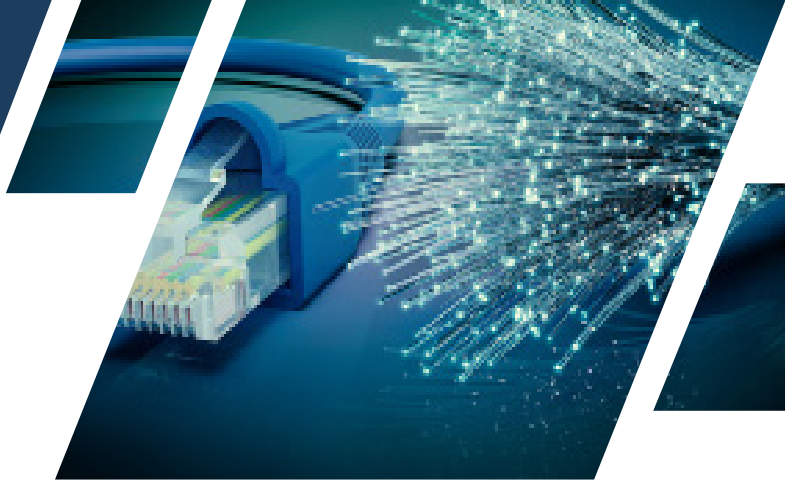
Ces attaques numériques, qui s'inscrivent dans le temps, nécessitent le plus souvent des capacités techniques élevées ainsi qu'une infrastructure complexe permettant aux attaquants de demeurer le plus discret possible. Ainsi, les architectures de sécurité doivent être non seulement cloisonnées et à jour des correctifs de sécurité, mais aussi faire l'objet d'une surveillance permanente. Pour les projets les plus sensibles, une interdiction des connexions à distance est fortement recommandée.

En ce qui concerne les systèmes d'information de niveau DIFFUSION RESTREINTE, les contrats doivent également prescrire, tout au long de la chaîne de sous-traitance, le respect des exigences de l'instruction interministérielle n°901[1] et prévoir des audits de sécurité des systèmes d'information réalisés par des prestataires de confiance.

.../...

[1] *Instruction interministérielle n°901 (www.ssi.gouv.fr)*

# Supply Chain



La sécurité de la chaîne de sous-traitance correspondant à celle de son maillon le plus faible, il est nécessaire, pour chaque sous-traitant, de procéder à l'homologation[2] de son système d'information dont la défaillance pourrait entraîner, outre l'exfiltration de données sensibles de ses clients ou l'interruption de ses activités, une atteinte à sa réputation et donc une perte d'activité.

## Pour une gouvernance de la SSI

Il revient alors à chaque acteur de la *supply chain* de mettre en place une véritable gouvernance de la SSI. Cette structure, chargée de piloter la politique de cybersécurité de l'entreprise, doit notamment cartographier les systèmes et données sensibles à protéger, puis évaluer les risques pesant sur ces actifs selon une méthodologie éprouvée. Face à chaque risque retenu, et de manière graduée, il convient ensuite d'identifier les contre-mesures techniques ou non adaptées, tout en veillant à intégrer des produits de sécurité qualifiés par l'ANSSI dans les architectures cibles.

C'est dans ce contexte que les sections zonales de contre-ingérence cyber de la DRSD, réparties sur l'ensemble du territoire, mènent régulièrement des actions de sensibilisation et de conseil en cybersécurité auprès des sociétés ayant des liens contractuels avec la Défense. Cette démarche d'homologation, qui traduit pour la direction de l'entreprise une acceptation du risque résiduel, constitue pour elle non seulement une "assurance-vie", mais également un avantage concurrentiel indéniable. ■

[2] *L'homologation en 9 étapes (www.ssi.gouv.fr)*

# Témoignage

## d'un officier de sécurité

Toute entreprise ou organisme titulaire d'un contrat avec le ministère des Armées (via la Direction générale de l'armement par exemple) est tenu d'appliquer les prescriptions réglementaires (IGI 1300) pour assurer la sécurité des informations ou supports classifiés (ISC) qui lui sont confiés. Afin d'élaborer et mettre en œuvre la politique de sûreté-sécurité, le représentant légal de l'entreprise désigne une ou plusieurs personnes à la fonction d'officier de sécurité.

Celui-ci doit disposer de tous les moyens nécessaires pour assurer ses missions, notamment l'organisation de la sécurité générale de l'entreprise, des relations avec le service enquêteur (la DRSD pour le ministère des Armées), les autorités d'habilitations et les autorités contractantes.

Le quotidien d'un officier de sécurité au sein de son établissement reflète la multitude de ses missions qui dépassent aujourd'hui largement la simple protection physique ou la gestion des intrusions de site.

Le contexte économique mondial, l'évolution rapide des technologies favorisant l'augmentation et la diversification des menaces et vulnérabilités potentielles confèrent en effet à l'officier de sécurité un rôle plus large et plus complexe. Ainsi, s'imposent à lui des capacités de détection, d'anticipation et d'analyse de l'environnement global de l'activité de l'entreprise afin de sécuriser le personnel, le patrimoine matériel et informationnel de celle-ci.

### Entretien avec Bernard Kass, officier de sécurité d'ArianeGroup (Saint-Médard-en-Jalles, Gironde)

**Les entreprises évoluent dans un monde complexe et incertain où se multiplient les risques et actes de malveillance. Comment définissez-vous votre rôle au sein de votre société ?**

Pour définir le rôle d'un officier de sécurité (OS), il faut au préalable resituer le contexte dans lequel il évolue et définir ce qu'est la SÉCURITÉ ainsi que la SÛRETÉ dans le milieu industriel.

A la différence de la sécurité, qui consiste à anticiper tout évènement involontaire (à l'image des accidents du travail, des pollutions, ...) qui, dans l'industrie, est plus généralement confiée à la Sécurité, la Santé et la protection de l'Environnement (SSE), la sûreté s'emploie, quant à elle, à prévenir tout acte volontaire pouvant déstabiliser ou rendre inopérante l'entreprise elle-même, que ce soit par des actions malveillantes, de l'ingérence, des tentatives d'espionnage industriel voire des actes terroristes.

En matière de sûreté, l'officier de sécurité d'un site se doit donc d'être un expert confirmé et un excellent conseiller des dirigeants. Il doit savoir gérer une crise, avoir une bonne connaissance des situations, posséder un excellent réseau de conseillers et d'experts ainsi que des contacts dans les services régaliens. Il doit également savoir piloter des recherches qui vont lui permettre d'avoir connaissance des incidents de sécurité même à l'extérieur et ce, toujours dans le strict respect de l'éthique et de la loi.

.../...

# Témoignage

## d'un officier de sécurité

De nos jours l'OS ne peut plus se permettre, comme par le passé, de se focaliser uniquement sur les méthodes d'intrusion, car son rôle ne consiste plus à tout fermer ou interdire les accès, mais plutôt à mettre en place des processus de gestion efficaces pour identifier et maîtriser les risques éventuels et résiduels.

Cet exercice est loin d'être aisé dans le contexte économique actuel où les exigences réglementaires et administratives ne cessent de croître tout comme le nombre de déplacements des personnels en raison de l'augmentation des contrats à l'international et des exigences de sûreté-sécurité réciproques que l'on impose à nos partenaires.

**Concernant la protection du secret dans les contrats d'armement, le rôle de l'OS est de veiller à la préservation des informations classifiées et/ou sensibles en veillant à faire appliquer les réglementations en vigueur. Pouvez-vous développer ?**

L'OS doit gérer et contrôler les droits d'accès aux informations et supports classifiés eux-mêmes (inventaires, récolements), mais également contrôler la bonne application des règles par l'ensemble des parties, qu'il s'agisse d'informations classifiées, confidentielles entreprises et/ou sensibles comme celles des savoir-faire technologiques.

Dans ce cadre, il doit savoir définir le besoin d'habilitation des personnels, afin que celles-ci ne soient pas distribuées à tout un chacun et ne deviennent pas des agréments de complaisance, ou servir comme filtre à l'embauche.

Il doit organiser des séances de sensibilisation régulières, afin que tous les salariés concernés bénéficient du même niveau de compréhension des risques et des menaces existantes ainsi que des règles applicables en matière de détention, d'accès et/ou de gestion des informations sensibles, que cela relève des informations et supports classifiés ou informations identifiées comme confidentiel entreprise.

Dans le cadre des contrats, l'officier de sécurité définit les mesures de protection préalables à la passation et à l'exécution des marchés et contrats, par la rédaction de clauses de protection qu'il rappelle à chaque acheteur ou chargé d'affaires pour qu'il les décline à tous les rangs de la sous-traitance.

Il constitue donc un acteur primordial dans la mise en place de contrats : il conseille toutes les parties sur les attendus en matière de prévention et de protection des informations stratégiques, sensibles ou classifiées.

Il travaille donc en étroite collaboration avec les acheteurs, les juristes, le service interne de contrôle-export, celui des douanes notamment lors de la signature des accords de non-divulgation (*Non-Disclosure Agreement*) ou encore d'engagements personnels de confidentialité soumis à chaque intervenant de la société sous-traitante retenue.

Les recommandations que promulgue l'officier de sécurité visent à sécuriser le patrimoine (produit, propriété intellectuelle, personnes) engagé durant toute la durée du contrat. Durant cette période, de nombreuses visites ou inspections sont programmées sur le territoire national ou à l'international afin de

.../...

# Témoignage

## d'un officier de sécurité

vérifier que les partenaires (clients, fournisseurs ou prestataires) veillent au respect des clauses contractuelles de sécurité (exemple : sanctuarisation de zones sensibles, limitation des accès à ces zones...).

De même, un rappel des règles de confidentialité à observer est dispensé auprès des donneurs d'ordre et chargés d'affaires, par le biais de sensibilisations régulières, notamment celle de rester particulièrement vigilant face à certains signaux faibles émanant de fournisseurs en situation monopolistique.

**Le rôle de l'officier de sécurité a donc évolué. Vos prérogatives couvrent-elles un spectre plus large ?**

Effectivement, notamment celui relatif à la protection du personnel lui-même, depuis la phase de recrutement, en relation étroite avec les services des Ressources Humaines, jusqu'à la mise en place de détection des signaux faibles en termes de vulnérabilités ou de subversion (interne/externe).

L'officier de sécurité gère également les flux des collaborateurs en mission en organisant très régulièrement des séances de sensibilisation ainsi que des rencontres individuelles notamment lors du processus d'habilitation.

Il doit également attacher une importance toute particulière à la protection des biens et des installations, en identifiant précisément les points névralgiques ou susceptibles d'intérêt, les savoir-faire de l'entreprise afin de sanctuariser les zones où ils sont situés. Cette réflexion conduit par exemple à l'élaboration d'un plan particulier de protection (PPP) ou encore d'un plan d'opération interne (POI) révisé annuellement et incluant des scénarii catastrophes.

La fuite de notre patrimoine intellectuel ou scientifique est, enfin, un sujet qu'on ne peut négliger, car elle est souvent le fait d'imprudences internes, lors de séminaires ou colloques, ou encore de certaines populations dites à risques comme les stagiaires, apprentis, alternants ou doctorants, lors de la rédaction de leurs rapports de stage, mémoires et autres thèses. Là aussi une relecture minutieuse s'avère indispensable avant toute diffusion. Elle s'effectue à quatre mains, d'abord par le responsable de la propriété intellectuelle et des brevets, puis par l'officier de sécurité qui en autorise la diffusion, parfois d'ailleurs assortie d'une soutenance à huis-clos lorsque la sensibilité du sujet l'exige.

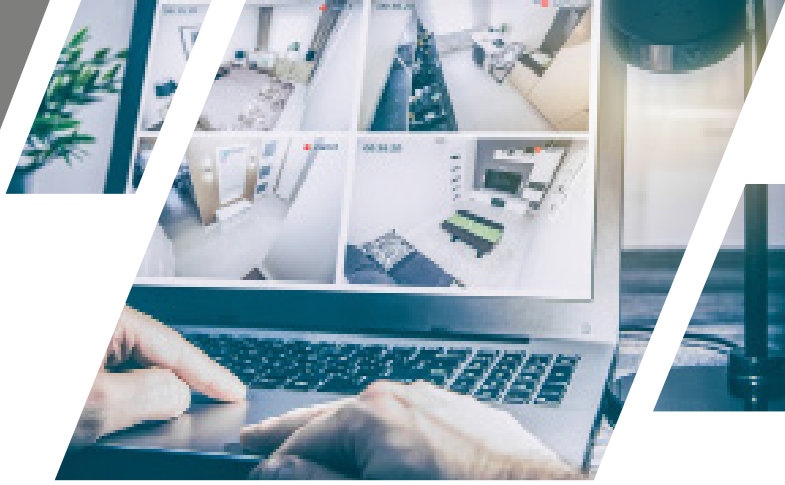
En la matière, notre entreprise s'est dotée d'une véritable politique de protection du patrimoine informationnel et des actifs immatériels en déterminant en amont ce qui doit être protégé par des droits d'auteur, des brevets ou placé sous licence *open-source*, mais aussi face aux risques induits par les médias sociaux, les voyages et les salons professionnels.

Des orientations ont également été prises quant aux nouvelles dispositions du secret des affaires, et donc à la divulgation d'informations qui pourraient compromettre gravement les intérêts de l'entreprise, en portant atteinte notamment à ses positions stratégiques, ses intérêts commerciaux et financiers et, bien sûr, sa capacité concurrentielle.

.../...

# Témoignage

## d'un officier de sécurité



**Qu'en est-il de votre rôle dans les programmes internationaux ?**

A l'image de programmes européens comme Ariane6, l'approche multinationale reste un véritable enjeu en matière de sûreté.

Désormais pleinement intégré dans une dynamique franco-allemande, ArianeGroup a désigné des référents sécurité en Allemagne. Ce sont eux qui assurent les relais en matière d'application des règles et protocoles élaborés par le siège social.

Les personnes désignées dans cette fonction occupaient déjà pour la plupart des fonctions identiques au sein des maisons mères et travaillaient de manière transverse avec la sûreté française. Nos procédures sont parfaitement claires et rodées. Tous ces éléments facilitent les échanges, permettent le partage et la mutualisation des bonnes pratiques tout en garantissant une déclinaison uniforme des procédures et exigences de sûreté-sécurité.

**Dans ce contexte de programmes internationaux ou simplement dans le cadre de déplacements à l'étranger, comment assurez-vous la sûreté-sécurité des collaborateurs en mission ?**

Face aux risques encourus par nos missionnaires et depuis la jurisprudence consécutive à l'attentat de Karachi ou « l'arrêt d'Abidjan », toute entreprise doit gérer la sécurité de ses employés en déplacement et notamment à l'étranger, ceci afin d'éviter la notion de "faute inexcusable" qui pourrait lui être reprochée.

Dans ce domaine, l'attentat terroriste n'est pas la seule menace à laquelle nos employés pourraient être exposés. Par exemple : les actes criminels crapuleux, le kidnapping, la prise d'otage, voire l'extorsion de fonds ou le péril sanitaire, sont des dangers pour lesquels l'entreprise doit également appréhender le coût du risque juridique, surtout s'il s'accompagne de conséquences médiatiques.

Pour y faire face ArianeGroup s'est doté d'une politique de sécurité en fonction du contexte international et géopolitique applicable à chaque missionnaire, dès lors que celui-ci quitte le territoire français et plus particulièrement s'il rejoint un pays à risque élevé.

Le plan d'action mis en place, témoignant de la sensibilité de l'entreprise face aux risques, s'est traduit par l'adoption d'une série de mesures :

- un circuit de validation hiérarchique. Un *Travel Manager* valide les déplacements ; un second *Travel Manager* valide les déplacements dans les pays à risques ;
- une formation aux risques spécifiques selon la nature de la mission, accompagnée d'un module de sensibilisation préalable à destination des voyageurs ;
- une souscription d'un contrat auprès d'un prestataire extérieur compétent dans le domaine, qui nous fournit en temps réel les alertes au niveau mondial. ■

# Contacts

*A venir :*

**Eurosatory**

8 au 12 juin 2020

Parc des expositions
Paris Nord Villepinte

93420 VILLEPINTE

Restons en contact

**Direction zonale Île de France**

prsd-villacoublay.cmi.fct@intradef.gouv.fr