



# LA LETTRE DE L'INTELLIGENCE ECONOMIQUE DU MINISTÈRE DE L'INTÉRIEUR

MISSION INTELLIGENCE ÉCONOMIQUE – SHFD

---

## *REVUE DE PRESSE*

### **INVESTISSEMENTS CHINOIS EN FRANCE : inauguration d'une usine de poudre de lait à Carhaix, en Bretagne, 28 septembre 2016, AFP.**

Avec 170 millions d'euros, l'usine de Carhaix constitue le plus gros investissement chinois à l'étranger dans la filière lait. Propriété du groupe SYNUTRA, elle vise la production, à terme, de 100 000 tonnes de poudre de lait par an à destination du marché chinois. Forte d'un contrat d'approvisionnement avec SODIAAL, première coopérative laitière en France, la société est en recherche de qualité et traçabilité pour ses produits, alors que la Chine doit faire face à une demande croissante et à des scandales sanitaires. Plusieurs groupes chinois ont ainsi investi dans des laiteries hexagonales comme à Montaigu en Vendée, à Isigny-Sainte-Mère en Normandie et désormais à Carhaix.

Le groupe compte poursuivre ses investissements à CARHAIX avec une usine dédiée au lait UHT.

## *L'ACTUALITE DE LA POLITIQUE PUBLIQUE D'IE*

### **Signature d'une convention relative à l'intelligence économique entre le ministère de l'intérieur et CCI-France.**

CCI-France et son réseau sont des partenaires quotidiens du ministère de l'intérieur et de ses coordonnateurs régionaux en matière d'intelligence économique. Bernard CAZENEUVE, ministre de l'Intérieur et André MARCON, président de CCI-France, ont signé une convention afin d'entériner ces relations, de généraliser et d'amplifier le partenariat entre le ministère et le réseau consulaire.

Cette convention a pour objet de favoriser l'échange d'informations et de bonnes pratiques en matière d'intelligence économique territoriale ainsi que de renforcer la capacité des préfets à mettre en œuvre la politique publique d'intelligence économique. Ce partenariat doit permettre de réaliser notamment des actions de sensibilisation et de formation.

Au ministère de l'intérieur, l'élaboration du texte a été coordonnée par le SHFD en collaboration avec la DGS, la DGGN, la DGPN et la DMAT.

Le texte de la convention et plus d'informations sur le site du SHFD : <http://shfd.minint.fr/>

## **Intelligence économique et normalisation.**

Le 27 septembre, le haut fonctionnaire de défense adjoint et la mission IE ont assisté à la première journée consacrée à la normalisation au ministère de l'intérieur.

Organisé par le responsable ministériel adjoint aux normes, Patrick BUTOR, et son équipe, ce séminaire a été ouvert par le secrétaire général, Denis ROBIN et a notamment abordé les enjeux majeurs que représente la normalisation en matière d'intelligence économique.

Pour plus d'information sur l'activité du ministère en matière de normes : <http://intranorme.sg.minint.fr/>

## **À LA RENCONTRE DES ENTREPRISES**

La gendarmerie diffuse actuellement un tryptique relatif à l'intelligence économique territoriale à destination des entreprises.

Il énonce les différentes missions de la gendarmerie en tant qu'acteur de la sécurité économique ainsi que les partenaires et points de contact.

Plus d'information page 3 et 4.

## **DOCUMENTATION D'INTELLIGENCE ECONOMIQUE**

Une synthèse intitulée « *intelligence économique et pôles de compétitivité : quelles perspectives internationales pour le modèle français ?* » a été rédigée par un des groupes de veille et analyse mis en place lors de la session nationale spécialisée 2015 – 2016 « *protection des entreprises et intelligence économique* » de l'INHESJ.

Après une étude comparative de ce phénomène dans 5 pays (Allemagne, Royaume-Uni, Etats-Unis, Japon et France), ce travail formule également des préconisations pour l'amélioration de l'efficacité des pôles et de la compétitivité française.

L'intégralité du document est consultable sur le site de l'INHESJ : <https://www.inhesj.fr/fr/content/les-travaux-des-auditeurs>.

*Pour plus d'informations, vous pouvez consulter notre site intranet :*

<http://shfd.minint.fr/index.php/intelligence-economique>

*Vous y trouverez notamment le plan triennal d'intelligence économique du Ministère de l'intérieur, le kit d'IE destiné au corps préfectoral, ainsi que nos dernières lettres d'intelligence économique.*



Lettre de l'intelligence économique : [abonnement](#) - [désabonnement](#)

# LES BONS RÉFLEXES

## En cas d'attaque de votre système d'information par un virus:

- isoler votre système d'information de l'internet (éteindre la box),
- identifier les postes touchés,
- procéder à la suppression du virus.

## En cas de blocage de votre système et de demande de rançon:

- ne pas payer la rançon,
- contacter les forces de l'ordre pour déposer plainte,
- faire appel à des techniciens pour débloquer le système.

## En cas d'intrusion de votre système d'information par un agresseur et de vol ou de modification de vos données:



- contacter les forces de l'ordre (gendarmarie ou police), qui pourront vous conseiller via leurs enquêteurs spécialisés (NTECH du réseau Cybergend ou ICC),
- isoler l'ordinateur concerné de votre système sans tenter de le rétablir,

- préserver les traces et indices laissés par l'attaquant,
- attendre l'intervention d'un technicien habilité dans le cadre de l'enquête.

## En cas de campagne de désinformation sur le web:

- analyser la source de la rumeur (concurrent, ancien employé, association...),
- éviter d'amplifier la rumeur par une réponse inadaptée,
- adopter une communication de crise.

## RÉFÉRENTS GENDARMERIE



Le dispositif qui regroupe les 2000 enquêteurs cyber de la gendarmerie (250 enquêteurs NTECH et 1700 correspondants-NTECH) est désormais fédéré sous l'appellation «CYBERGEND». Ce réseau décentralisé assure un maillage sur tout le territoire national, aussi bien en métropole qu'outre-mer. Il constitue un ensemble de points de contact et de capacité d'action de proximité, doté de véritables capacités d'investigations. Il est piloté par le centre de lutte contre les cybercriminalité numérique (C3N) de Pontoise.



Déployés dans l'ensemble des départements, en métropole et en outre-mer, les 234 référents sûreté de la gendarmerie agissent quotidiennement au profit des entreprises. Au-delà de leur expertise dans la prévention technologique de la malveillance, les référents sûreté peuvent conseiller sur les mesures de protection à mettre en œuvre pour lutter contre la cyberdélinquance et orienter les chefs d'entreprise vers les référents intelligence économique des régions ou le cas échéant, vers les enquêteurs du réseau Cybergend.

## CONTACTS

Pour aller plus loin ou obtenir de l'information:

[www.gendarmerie.interieur.gouv.fr](http://www.gendarmerie.interieur.gouv.fr)



[www.ssi.gouv.fr](http://www.ssi.gouv.fr)

Pour signaler:

- des piratages dans une entreprise: [cyber@gendarmerie.interieur.gouv.fr](mailto:cyber@gendarmerie.interieur.gouv.fr)
- des contenus illégaux sur Internet: <https://www.internet-signalement.gouv.fr>
- des courriels ou sites d'escroqueries: <https://www.internet-signalement.gouv.fr> ou 0811 02 02 17
- des spams: <https://www.signal-spam.fr/>
- des sites de phishing: <http://www.pishing-initiative.com/>

## EN CAS D'URGENCE, COMPOSEZ LE 17

Votre point de contact local?

Selon la gravité de votre incident, ce point de contact local sera en mesure de faire intervenir des enquêteurs spécialisés en cybercriminalité.

COORDONNÉES DE VOTRE CONTACT LOCAL

GENDARMERIE NATIONALE

# LA GENDARMERIE S'ENGAGE

## CYBERMENACES COMMENT PROTÉGER VOTRE ENTREPRISE?



**- SCÈNE CYBERCRIME -**  
**GENDARMERIE NATIONALE - SCÈNE**



MINISTÈRE  
DE  
L'INTÉRIEUR



Votre entreprise est "connectée" : Site internet, page Facebook, smartphone mais aussi correspondance électronique qui contient souvent des données confidentielles. Internet est devenu un outil incontournable. Facteur de croissance et de développement, il peut aussi être source de vulnérabilités majeures.

Les cybercriminels s'intéressent à tout ce qui fait la valeur de votre entreprise et tentent de procéder à de faux ordres de virements: fichiers clients, réponses à des appels d'offres, données personnelles de vos salariés ou de vos fournisseurs. La protection face aux cybermenaces est une priorité stratégique pour protéger ce qui fait la richesse de votre entreprise.

*Prenez le temps de lire ces quelques conseils. Quelle que soit la taille de votre entreprise, vous êtes concerné.*

## CYBERMENACES: 3 RISQUES MAJEURS POUR L'ENTREPRISE

### RISQUE ÉCONOMIQUE

**Le vol de savoir-faire et de données commerciales.** Exemple: Un virus introduit par une pièce jointe piégée ouvre les portes de vos systèmes vers l'extérieur et permet à un concurrent de voler votre plan de développement à 5 ans.

**Des pertes d'exploitation suite à une prise en otage de votre système d'information.** Exemple: un virus de type rançongiciel bloque votre ordinateur en faisant apparaître un écran simulant un service étatique (police, gendarmerie) et vous menace de poursuites si vous ne payez pas une amende.

**L'interception de données confidentielles (contacts, mail, mots de passe) lus sur des supports mobiles (smartphone, tablette, etc.).** Exemple: vous connectez votre tablette sur un WiFi public pour finaliser une proposition commerciale: votre échange peut être intercepté par un concurrent.

### RISQUE D'IMAGE

L'image de votre société peut être directement touchée par une campagne de dénigrement propagée sur le Net. Exemple: Dénigrement de votre entreprise sur des médias sociaux par des concurrents ou des salariés mécontents entraînant une perte de confiance de vos clients et fournisseurs.

### RISQUE JURIDIQUE

Votre responsabilité civile et pénale est engagée si vous n'avez pas protégé juridiquement vos données et si vous n'avez pas mis en œuvre les moyens à l'état de l'art pour les protéger. Exemple: votre charte interdit la navigation sur des sites présentant des contenus illégaux: Avez-vous mis un filtre URL pour le contrôler?

## NOS CONSEILS PRATIQUES À METTRE EN ŒUVRE DÈS AUJOURD'HUI...

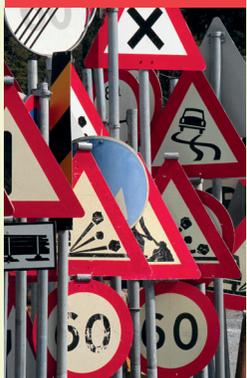
#### ACTION n°1



### SENSIBILISER VOS COLLABORATEURS

- Sensibiliser vos collaborateurs à la **discrétion lors de leurs déplacements** (aéroports, hôtels) et aux règles de protection de leurs équipements mobiles. Apporter une attention particulière en cas de déplacement dans certains pays étrangers. *S'aider pour cela du Passeport de conseils aux voyageurs de l'ANSSI.*
- **Identifier les informations sensibles** et former vos collaborateurs à ne pas les diffuser sur les réseaux sociaux.
- Prendre des précautions adaptées lors de visites extérieures (exemple: pas d'accès à un ordinateur raccordé au réseau dans la salle de réunion)
- Vérifier régulièrement **l'image de votre entreprise sur internet** (e-reputation)

#### ACTION n°2



### FIXER DES RÈGLES POUR L'UTILISATION DU SYSTÈME D'INFORMATION

- Adopter une **charte informatique** définissant les droits et devoirs des personnels (salariés, stagiaires, intervenants externes...). Cette charte doit clairement énoncer les sanctions encourues en cas de non-respect des règles. *Exemple de charte informatique disponible sur le site de la gendarmerie.*
- Impliquer direction générale et DRH dans les processus de mutation et de départ de collaborateurs. (exemple: suppression immédiate des droits d'accès suite à la mutation ou au départ d'un collaborateur).
- Faire signer des clauses de confidentialité à vos prestataires ou personnels temporaires (stagiaires). *Exemple de clause de confidentialité disponible sur le site de la gendarmerie.*

#### ACTION n°3



### LA SÉCURITÉ DU SYSTÈME D'INFORMATION

- Faire **le bilan, avec votre responsable informatique**, de la situation de votre entreprise sans oublier les terminaux mobiles en vous aidant du guide d'hygiène informatique de l'ANSSI et des recommandations de sécurité relatives aux ordiphones.
- Effectuer des **sauvegardes régulières** de vos données et tester leur récupération.
- Définir vos **procédures de reprise d'activité** en cas de destruction totale de votre système d'information (incendie, crue...). Envisager éventuellement la souscription d'une assurance contre les pertes d'exploitation.