Masterclass - Aliptic - Limoges (08/12/2022)

Le dispositif de la PPIE

Politique publique d'intelligence économique

En France

PRESENTATION

Intervenante : Elysabeth Bénali-Léonard

- Présidente SAS ExAcT international

IHEMI
INSTITUT DES HAUTES ÉTUDES DU MINISTÈRE DE L'INTÉRIEUR

- Expert en Protection des Entreprises & Sécurité Economique
- Conseillère du Commerce Extérieur de la France
- Déléguée S Y N F I E
- Membre Comité Afnor CN Cyber

cce
Comité national des conseillers du commerce extérieur de la France

PRESENTATION

ExAcT international sas –
Technopole Ester – LIMOGES – France.

Métiers

- **1. AUDIT de SECURITE ECONOMIQUE**
- **2. PREVENTION et RESILIENCE en cas de CYBERATTAQUE**
- **3. DEVELOPPEMENT INTERNATIONAL /INFLUENCE**
- **4. SEMINAIRES**

POURQUOI une PPIE ?

ATTAQUES contre les INTERETS ECONOMIQUES Français

Investissements étrangers en France (IEF) :
Rachats d'entreprises technologiques

Utilisation du droit comme arme économique
Pillage d'informations, amendes colossales (FCPA)

Souveraineté numérique
Règlement Européen sur la protection des données RGPD 2016 vs
CLOUD Act américain 2018

Cyberattaques

POURQUOI une PPIE ?

CONSEQUENCE :

Une FRAGILISATION des ACTEURS ECONOMIQUES

UNE PERTE DE SOUVERAINETE

DE NOTRE PAYS

QUI PILOTE ?

Le SGDSN = Secrétariat Général à la Défense et la Sécurité Nationale (sous l'Elysée)

MINISTERE de l'ECONOMIE

MINISTERE de l'INTERIEUR

MINISTERE des ARMEES

S I S S E

Service de l'Information Stratégique et de la Sécurité Economique

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

RÉPUBLIQUE FRANÇAISE · DIRECTION GÉNÉRALE DE LA SÉCURITÉ INTÉRIEURE · DGSI

Gendarmerie nationale

DIRECTION DU RENSEIGNEMENT ET DE LA SÉCURITÉ DE LA DÉFENSE · DRSD

QUI PILOTE ?

PREFECTURE

Disse Dtsi — Opérateur d'Importance Vitale - O I V

Disse Dtsi — Service d'Activité d'Importance Vitale - SAIV

Disse Dtsi — Patrimoine scientifique et Technique de la Nation - PPST

SECURITE ECONOMIQUE = REGALIEN (compétence unique de l'Etat)

COMMENT ?

LA POLITIQUE PUBLIQUE D'INTELLIGENCE ECONOMIQUE doit :

- Garantir la continuité de l'activité économique en cas de crise majeure.
- Assurer la protection des intérêts économiques de la Nation.
- Organiser l'approvisionnement et l'utilisation des ressources nécessaires à la défense et à la sécurite nationale.
- Détecter et prévenir les menaces susceptibles d'affecter les entités économiques sensibles (OIV/SAIV).

QUELLES CIBLES en PRIORITE :

LES CIBLES d'INTERET VITAL pour la nation :

Appelés OPERATEURS d'IMPORTANCE VITALE = OIV

Regroupés en 4 grands services d'activités = SAIV

- TECHNOLOGIQUE
- ECONOMIQUE
- REGALIEN
- HUMAINE

QUELLES CIBLES en PRIORITE :

1. ALIMENTATION – GESTION de L'EAU - SANTE

2. ACTIVITES CIVILES et JUDICIAIRES
   ACTIVITES MILITAIRES de l'ETAT

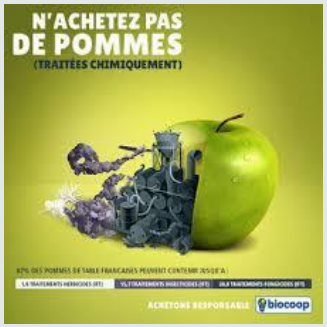
3. ENERGIE
   FINANCES
   TRANSPORT

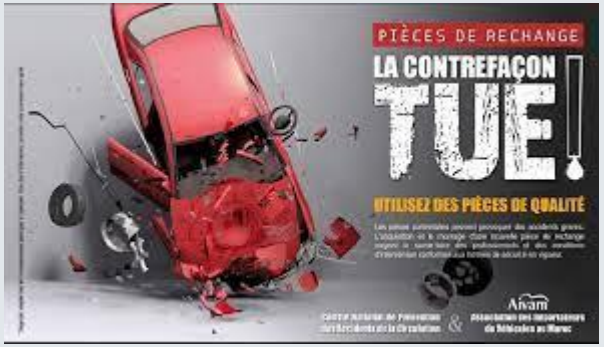
4. AUDIOVISUEL et INFORMATION
   COMMUNICATIONS ELECTRONIQUES
   INDUSTRIE
   ESPACE ET RECHERCHE

EXEMPLES D'ATTEINTES ECONOMIQUES :

Cyberattaques : phising, DNS..

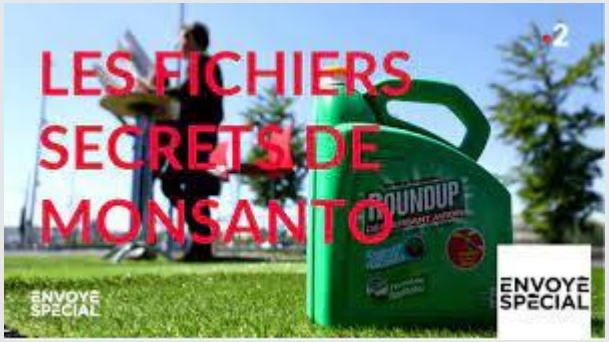
Dénigrement

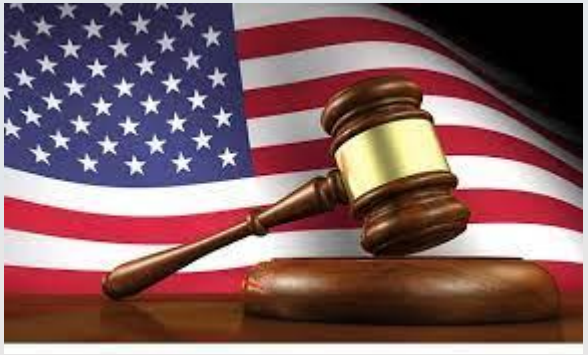




Contrefaçon

Lobbying





IEF
FCPA..

OBLIGATIONS des O.I.V. (Opérateurs d'Importance Vitale)

Mettre en place une sécurité économique dans l'entreprise pour assurer sa resilience :

- Sécurité des systèmes d'information (stratégie, organisation, protection)
- Plan de continuation d'activité (PCA) en cas de cyberattaque
- Politique de conformité avec les partenaires(Due diligence/compliance)
- Sécurité physique et contrôle d'accés

ARSENAL LEGISLATIF FRANCAIS et EUROPEEN

RGPD	Lois SAPIN I et 2	Loi PacTe	Loi Secret des Affaires	Loi de Blocage IEF	Loi protection lanceurs d'alerte
UE 2016 - Préserver la vie privée - Maitriser le contrôle de la data;	Fr 1993/2016 - Prévention corruption et transparence de la vie Publique - Protéger Lanceurs d'alerte	Fr 2019 - IEF soumis à autorisations (secteurs stratégiques) - Décret Montebourg 2014+2019	UE 2016 Fr 2018 - Protéger contre l'espionnage industriel, - Renforcer propriété intellectuelle	Fr 1968/2022 - Empecher de communiquer des infos stratégiques à des personnes étrangères	UE 2019 Fr 2022 - Divulgation de bonne foi d'infos sur une menace pour l'intérêt général
Cloud Act 2018	Obligation Ets>500 salariés				

QUELQUES POINTS DE CONTACTS APRES L'ATTAQUE :

CYBERATTAQUES

OIV et SAIV

COLLECTIVITE *ENTREPRISE*

Contactez l'ANSSI

Agence Nationale de Sécurité des Sytèmes d'Information

https://www.ssi.gouv.fr/en-cas-dincident/

POINT de CONTACT

PARTICULIER

Victime d'une Cyberattaque ?
ContacteZ le dispositif d'assistance CYBERMALVEILLANCE :
https://www.cybermalveillance.gouv.fr

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Vous souhaitez signaler un contenu illicite ou représentant une menace ?
Connectez vous sur le site PHAROS :
https://www.internet-signalement.gouv.fr/PharosS1/

PHAROS
PLATEFORME D'HARMONISATION, D'ANALYSE, DE RECOUPEMENT ET D'ORIENTATION DES SIGNALEMENTS

ATTAQUE ECONOMIQUE :
DENIGREMENT / LOBBYING / CONTREFACON

https://sisse.entreprises.gouv.fr

SISSE

Votre situation concerne un sujet économique ou scientifique : securite-economique@interieur.gouv.fr

Votre situation vous fait craindre une potentielle ingérence étrangère :
assistance-dgsi@interieur.gouv.fr

ATTAQUE ECONOMIQUE :
DENIGREMENT / LOBBYING / CONTREFACON

Votre entreprise fait l'objet d'une campagne de dénigrement ?

Vous ne voulez pas disparaitre après une cyberattaque ?

Faut-il breveter votre innovation ?

Comment s'assurer de la fiabilité d'un partenaire ?

Contactez nous : info@exact-international.com

...FIN

MERCI DE VOTRE ATTENTION