



FORMATION WEBEX IKARIAN 2020

Dans le contexte de choc économique dû au COVID-19
**COMMENT PROTÉGER VOTRE ENTREPRISE
DES TENTATIVES DE DÉSTABILISATION ET
DE PRISE DE CONTRÔLE HOSTILES ?**

Module 1 :
L'angle d'attaque financier et capitalistique

JEUDI 18 JUIN

de 9h à 12h30

Module 2 :
L'angle d'attaque réputationnel, juridique et
numérique

MARDI 07 JUILLET

de 9h à 12h00

LE CONTEXTE :

La crise sanitaire et économique actuelle met à mal les modèles économiques, les finances, la trésorerie des entreprises, leurs valorisations ainsi qu'éventuellement l'équilibre et la stabilité de leur actionnariat.

Elle aiguise des appétits de la part de concurrents de plus en plus fréquemment épaulés voire guidés par leurs Etats.

Dans ce contexte, il importe pour chaque entreprise de se préparer contre de telles manoeuvres hostiles et donc de savoir détecter ces agissements nuisibles dès l'amont, d'avoir une compréhension de leurs modes opératoires afin de mieux les anticiper, puis d'identifier et de désamorcer ses propres points de faiblesse.

OBJECTIFS DE LA FORMATION :

Comprendre les modes opératoires récurrents des diverses formes d'attaques financières et capitalistiques.

Savoir évaluer le degré d'exposition et de besoin de protection d'une entreprise.

Modalité d'évaluation des acquis

Les acquis de la formation ne font pas l'objet d'une évaluation formalisée des connaissances. Il est demandé aux participants d'évaluer la qualité de la formation sous forme d'un questionnaire de satisfaction à l'issue de la formation

DURÉE D'UN MODULE DE LA FORMATION : 3H00

PUBLIC

Actionnaires, administrateurs, dirigeants, responsables des risques et autres cadres de tout type d'entreprises cotées ou non (grandes entreprises, ETI, Start-up, fonds d'investissement, LBO, banques d'investissement).

PRÉREQUIS

Aucun

PROGRAMME MODULE 1

L'ANGLE D'ATTAQUE FINANCIER ET CAPITALISTIQUE

Introduction : Premier contact avec une réalité concurrentielle sous-estimée

Déstabilisations d'entreprises et captations de leurs patrimoines

- ▶ Acteurs impliqués et motivations (entreprises, officines de renseignement financier et d'intelligence économique, agences d'Etat...).
- ▶ Les relais nationaux fréquemment mobilisés ou à l'origine de ces opérations : liaisons et alliances prédatrices entre bénéficiaires privés et organismes d'Etats, parfois jusqu'aux milieux criminels.
- ▶ Leurs moyens et leurs principaux modes opératoires. Quelle défense reste possible au vu de ces moyens ?
 - Sur l'information sensible
 - Sur la structure interne ainsi que sur l'environnement de l'entreprise avec ses réseaux
- ▶ Comprendre les tempos et le cadencement de ces opérations.
- ▶ Typologie des diverses formes de déstabilisation : contre la cohésion, la réputation, l'information des entreprises, etc.

L'affaire « Gemplus »

- ▶ Témoignage exceptionnel de Marc Lassus qui expliquera comment « Gemplus », leader mondial de la carte à puce et qui comptaient plus de deux milliards d'utilisateurs dans le monde au début des années 2000, a subi un raid orchestré par les services américains.

Les angles d'attaque potentiels

- ▶ Identification des éléments vitaux de chaque entreprise, et de sa position sur le terrain concurrentiel.
- ▶ Grille d'analyse de l'exposition et des fragilités de chaque entreprise (carence en CA, en trésorerie, vis-à-vis des tiers - fournisseurs, clients -). Prise en compte des protections déjà en place (sur l'organisation, les communications...) :
 - Le capital et/ou l'actionnariat des entreprises visées
 - Les capacités financières de ces entreprises
 - Leur chaîne logistique, et leurs partenariats externes
- ▶ Savoir cartographier les risques (stratégiques, opérationnels, financiers) en vue de mieux détecter et collationner les signaux faibles, pour une lecture précoce de la menace.
 - Validité de la cartographie (évaluation, probabilité, vraisemblance, types d'erreurs...)
 - Risques de détournement et signaux d'alerte
- ▶ Faut-il créer une nouvelle fonction temporaire ? Qui et comment doit faire l'analyse des fragilités et porter le problème ?

PROGRAMME MODULE 2 L'ANGLE D'ATTAQUE RÉPUTATIONNEL, JURIDIQUE ET NUMÉRIQUE

Introduction : Vers une accélération des pratiques de déstabilisation économique

L'angle d'attaque juridique et réputationnel : des enjeux majeurs et stratégiques pour l'entreprise

- ▶ Utilisation de la loi comme outil de pression économique
 - Les lois extraterritoriales américaines et anglaises (FCPA, UKBA, Export Control, sanctions économiques) et autres (False Claim Act)
 - Vers une nouvelle vision des lois extraterritoriales en Asie?
- ▶ Les moyens utilisés et les scénarios de déstabilisation : ne pas devenir une cible facile.
 - Les stratégies mises en oeuvre
 - Etude de cas réels
- ▶ Les conséquences sur l'entreprise visée
 - Déstabilisation de la structure managériale
 - L'enquête interne : coûts et conséquences
 - La responsabilité pénale des dirigeants et conflits d'intérêts
 - L'impact réputationnel et ses conséquences financières
- ▶ Les réponses : comment prévenir et se défendre ?
 - Au niveau de l'entreprise visée (enjeux internes de gestion et mise en place des procédures)
 - Au niveau français et européen

L'angle d'attaque numérique : batailles normatives dans le Cyberespace : renseignement électronique, RGPD et Cloud Act

- ▶ Digitalisation de l'activité économique comme vecteur de création de nouveaux espaces de vulnérabilités
- ▶ Le Cyberespace en voie d'appropriation par les grandes puissances pour capter les informations stratégiques : la course au renseignement électronique.
- ▶ Les réglementations numériques et conflits normatifs
 - US Cloud Act vs exigences du RGPD européen
 - Le futur du règlement européen « E-Evidence »
 - Le Corporate « Social Credit System » en Chine
 - Embargos de l'Occident contre la 5G en Chine
- ▶ Etude des réglementations numériques pesant sur les entreprises et susceptibles d'être sources d'intrusion et de déstabilisation.
- ▶ Adopter les bonnes pratiques curatives de cyber sûreté et de sécurité des données.

INTERVENANTS MODULE 1

L'ANGLE D'ATTAQUE FINANCIER ET CAPITALISTIQUE



Marc LASSUS

Ingénieur (INSA) et docteur en physique des solides, il fonde en 1989 avec quatre ingénieurs de Thomson, la société Gemplus qui deviendra n°1 mondial des cartes à puce et réalisera jusqu'à 1,2 milliard d'euros de chiffres d'affaires. L'affaire « Gemplus » est considérée comme un véritable cas d'école en matière de guerre économique moderne et d'intelligence économique.

L'entreprise, numéro un mondial de la carte à puce devant SchlumbergerSema, Oberthur Card Systems et Giesecke & Devrient est victime, au début des années 2000, d'un espionnage économique intense puis d'une prise de contrôle par les services de renseignement américains.

Aujourd'hui, Marc Lassus est conseiller stratégique de multiples entreprises et spécialiste en coaching en entreprises émergentes dans le secteur des technologies renouvelables, technologies NFC, objets connectés et informatique.



Philippe LAURIER

Chercheur en intelligence économique, notamment sur les déstabilisations d'entreprises et la protection de leur patrimoine, ainsi que sur l'évaluation des préjudices engendrés par les attaques informatiques.

Son parcours associe les deux composantes complémentaires de l'intelligence économique (l'attaque) et de l'innovation (une cible). Actuellement responsable du séminaire « Intelligence économique » à l'Ecole Polytechnique ainsi que de modules sur ces sujets à Dauphine et Paris 1 Sorbonne, il enseigne également à l'École des Ponts et Chaussées, à l'Ecole des Mines de Paris, à l'ENSTA, à l'ESIEA et à Télécom Paris.

Il a monté l'incubateur de jeunes entreprises innovantes devenu depuis lors ParisTech Entrepreneurs, et a été responsable de modules sur l'innovation à Télécom Paris, à l'université de Compiègne (UTC) ainsi qu'à l'ENSEA. Auteur d'une dizaine de livres notamment sur l'intelligence économique, sur l'innovation et la création d'entreprises technologiques, il est également docteur en économie.





Frédéric PIERUCCI

(MSc ENSMA, MBA Columbia Business School), est un ancien cadre dirigeant d'ALSTOM ayant une grande expérience internationale puisqu'il a vécu et travaillé en Chine, aux Etats-Unis, en Algérie, au Royaume-Uni, à Singapour et en France. Jusqu'à la mi-2013, il dirigeait depuis Singapour le business « Chaudières » (ALSTOM Boilers) représentant 1,4 M€ de CA et 4 000 employés.

Lors d'un voyage d'affaires aux États-Unis en 2013, il a été arrêté par le FBI à l'aéroport de JFK alors qu'il descendait de l'avion, accusé « d'avoir participé à des faits présumés de corruption en Indonésie dans le cadre d'un contrat qu'ALSTOM a obtenu en 2003 ».

Fort de cette expérience unique, il a créé en 2015 IKARIAN, une société de conseil dont le but est d'assister et de conseiller ses clients sur les défis auxquels les entreprises et leurs dirigeants sont confrontés pour se conformer au Foreign Corruption Practice Act (FCPA), au UK Bribery Act (UKBA), à la loi « Sapin 2 » et à d'autres lois ou normes anticorruption telles que l'ISO 37001. IKARIAN a développé une approche unique de la conformité en combinant l'expertise de cadres internationaux de haut niveau, de professionnels de l'intelligence économique et, si nécessaire, d'experts juridiques. IKARIAN conseille les grandes et moyennes entreprises en France et à l'étranger.

Frédéric est l'auteur, avec le journaliste Matthieu Aron, du best-seller « Le Piège américain » (Editions JC Lattès, janvier 2019) traduit en anglais sous le titre « The American trap » (Hodder & Stoughton, novembre 2019)



Noël PONS

Expert international et Instructeur (prévention, cartographie des risques, investigation) en fraudes, corruption, blanchiment et criminalité organisée, ainsi qu'en matière d'audit et d'investigation comptable.

Noël Pons est ancien conseiller au Service central de prévention de la corruption et inspecteur des impôts. Aujourd'hui, il est membre de L'Institut Français de l'Audit Interne et il partage son expérience en tant que formateur IFACI et ELEGIA. Il est co-directeur pédagogique des certificats fraude et corruption de l'École supérieure de la sûreté des entreprises (ESSE).

Noël Pons est essayiste, auteur notamment de « Audit et fraudes », « Cols blancs et mains sales - Économie criminelle, mode d'emploi », « L'investigation informatisée des fraudes - Recherche informatisée et prévention », « La corruption des élites », « 92 Connection » et « Histoire secrète de la corruption sous la Vème République (ouvrage collectif) ».

INTERVENANTS MODULE 2 L'ANGLE D'ATTAQUE RÉPUTATIONNEL, JURIDIQUE ET NUMÉRIQUE



Olivier de MAISON ROUGE

Avocat d'affaires spécialiste du droit de l'intelligence économique. Docteur en droit. Diplômé de Sciences politiques.

Olivier de Maison Rouge est professeur associé à l'Ecole des relations internationales (ILERI), intervenant à l'INHESJ, à l'IHEDN, à l'Ecole Nationale de la Magistrature (ENM) et à l'Ecole de Guerre Economique (EGE) au sein du MBA de Management des risques, sûreté internationale et cybersécurité (MRISC). Il est également vice-président de la Fédération européenne des experts en cybersécurité.

Membre de la commission permanente « secrets d'affaires » de l'Association Internationale pour la Protection de la Propriété Intellectuelle (AIPPI), Olivier de Maison Rouge est également Président du comité d'éthique du syndicat français de l'intelligence économique (SYNFIE).

Olivier de Maison Rouge est l'auteur des ouvrages suivants :

- « Les Cyberisques » LexisNexis, 2018 ;
- « Penser la guerre économique. Bréviaire stratégique. » VA Press, 2018 ;
- « Le droit du renseignement - renseignement d'Etat, renseignement économique », LexisNexis, coll. Actualité, 2016 ;
- « Le Droit de l'intelligence économique. Patrimoine informationnel et secrets d'affaires », Lamy, coll. Axe Droit, 2012.



Ali LAIDI

Chercheur à l'Ecole de pensée sur la guerre économique (EPGE), docteur en science politique, Ali Laïdi est l'auteur de nombreux ouvrages de référence dans le domaine de la guerre économique :

- « Les secrets de la guerre économique », Seuil, 2004
- « Retour de flamme. Comment la mondialisation a accouché du terrorisme », Calmann-Lévy, 2006 ;
- « Les Etats en guerre économique », Seuil, 2010, Prix Turgot IES 2010 ;
- « Aux sources de la guerre économique », Armand Colin, 2012 ;
- « Histoire mondiale de la guerre économique », Perrin, 2016.
- « Le droit, nouvelle arme de la guerre économique », Actes Sud, 2019, Grand Prix du jury Turgot 2020, Prix Etudiant HEC/Manpower.

Il est également chroniqueur à France 24, responsable de « L'Entretien de l'Intelligence économique ».

Frédéric PIERUCCI interviendra lors du Module 2 de la formation.

CONTACT POUR LES INSCRIPTIONS :

akorn@ikarian.eu ou par téléphone au **+33 (0)6 03 99 34 69**

La formation se tiendra sous forme du webinar, le lien de connexion sera envoyé aux participants suite à l'inscription.

TARIF :

280 Euros HT - 336 Euros TTC *



* Notre cabinet est certifié organisme de formation, enregistré sous le numéro : 11 75 54409 75 auprès de la préfecture d'Ile de France, le coût de chaque session de formation pourra ainsi s'imputer sur le budget de formation des entreprises tel que prévu par le Code de Travail.

MODES DE RÈGLEMENT

Par chèque

► À l'ordre de **IKARIAN** en portant la mention au dos du chèque la date de la formation et le nom du/de la participant(e).

À adresser à IKARIAN, 3, rue de Téhéran, 75008, Paris.

► IBAN : FR76 3000 4001 7800 0104 1667 192

BIC : BNPAFRPPXXX

Domiciliation : BNP PARIBAS

Titulaire du compte : IKARIAN

Insérer dans le libellé la mention de la date de la formation et le nom du/de la participant(e).