Le secteur français de l'industrie de défense face aux risques informationnels

EGE Ecole de Guerre Economique

Sous la direction de
Christian Harbulot

Ana-Maria BAGNATO
Sophie CASUCCINI BONCI
Hippolyte CHANTEUR
Paul-Erwan DE BUTLER
Gauthier LARIVIERE
Morgane LE COGUIC
Manon LEMERCIER
Sarah MARÉCHAL

Table des matières

Introduction

« *Le risque est désormais beaucoup plus qu'une menace : il est devenu la mesure de notre action.* »[1] Les propos d'Ullrich Beck retiennent toute notre attention dans le cadre de cette étude. Aujourd'hui, les nouveaux risques sont de nature informationnelle ou cognitive, concrétisés par des atteintes à la réputation des entreprises. La mise en cause de la responsabilité sociétale d'une entreprise et sa médiatisation apparaissent comme un révélateur d'attaques informationnelles élaborées à l'aide d'interception d'information ou de désinformation. L'accès grandissant aux technologies de la communication dans le domaine économique favorise la diffusion intentionnelle d'informations, qu'elles soient vraies, fausses ou erronées. Cette propagation de connaissances survient dans le but délibéré de nuire à la réputation d'une entreprise afin de remettre en cause sa crédibilité auprès de ses clients ou de ses partenaires. Cela peut venir aussi bien d'un client de l'entreprise, d'un intermédiaire commercial, d'un concurrent ou d'un lobby. Les *fake news*, notion qui a émergé ces dernières années, sont une parfaite illustration d'attaque par le contenu.

Ces dernières années, l'attaque informationnelle sur l'industrie de défense française a pris une ampleur sans précédent. Sa vulnérabilité face au risque réputationnel rend en effet possible la manipulation de l'information pour porter atteinte à son intégrité.
Le secteur de l'armement français représenterait une cible idéale : troisième exportateur mondial derrière les États-Unis et la Russie, la France fournit les principaux pays importateurs d'armes (Arabie Saoudite, Inde, Égypte, Australie). Elle se démarque avec deux contrats emblématiques remportés respectivement en 2012 et 2016, en Inde (36 Rafale par Dassault Aviation) et en Australie (12 sous-marins de type Barracuda par Naval Group). L'insolente croissance[2] de l'armement *Made in France* depuis les années 2010 survient dans un contexte de concurrence particulièrement vive avec la volonté de suprématie américaine et l'émergence de nouveaux grands exportateurs telle que la Chine.

De fait, le secteur de la défense ne présente pas les caractéristiques de la « concurrence pure et parfaite » : le rôle central des États en tant qu'acheteurs et la nature sensible des produits en font une industrie aux normes particulières. Les exportations d'armement sont fortement réglementées et les principes du libre-échange ne s'y appliquent pas, ce dont témoigne d'ailleurs l'exclusion des produits militaires des règles de l'OMC[3].
Par ailleurs, les grandes multinationales de l'armement mettent en place des stratégies industrielles caractéristiques des secteurs à forte valeur ajoutée et à haute sophistication technologique, avec la création de partenariats avec des concurrents, à travers des filiales ou des *joint-ventures* à l'étranger pour mieux pénétrer certains marchés. L'industrie mondiale de l'armement est par conséquent définie aujourd'hui par un double mouvement de compétition et de coopération.

[1] Ullrich BECK, ''La société du Risque'', *Alto (Aubier)*, EAN 9782700736793, 25/10/2001.
[2] Les ventes d'armement français ont augmenté de 72 % par rapport à la période 2010-2014, pendant laquelle la part de marché de la France atteignait 4,8 %. Ce bond spectaculaire reflète les succès commerciaux de Dassault Aviation en Égypte et en Inde pour le Rafale ou encore ceux de Naval Group au Brésil et en Inde pour des sous-marins, en Égypte, en Malaisie et aux Émirats arabes unis pour des frégates
[3] Fanny COULOMB, ''Industries de la défense dans le monde'', *PUG*, 2017.

En outre, les barrières à l'entrée dans ce secteur sont très élevées : il s'agit d'un marché caractérisé par un petit nombre de vendeurs face à un grand nombre d'acheteurs. De même, à l'heure de la tumultueuse mise en place de l'Europe de l'armement, les industriels français doivent compenser par leurs exportations l'important différentiel entre les crédits européens et les budgets américains. La concurrence est donc acharnée dans un secteur qui fait figure de « famille » où tout se sait : certains acteurs étant partenaires à l'échelle nationale, mais concurrents à l'échelle internationale ou inversement, l'information circule très rapidement entre les parties prenantes.

Dès lors, au cours de la seule année 2020, la condamnation d'Airbus pour corruption, la campagne malveillante contre Naval Group à l'œuvre en Australie, ainsi que la modification de la norme ITAR visant à la rendre plus contraignante ne sont pas anodines. L'étau se resserre autour de l'industrie de défense française, dont les actions semblent se dérouler de plus en plus sous le feu des projecteurs. Les enjeux du secteur peuvent ainsi être résumés par les questions suivantes : quels sont les leviers d'attaque par le contenu activables pour entraver la réputation d'une entreprise de défense ? Quels effets produisent les attaques par la désinformation, la rumeur ou la polémique sur le fonctionnement global du secteur ? Quels sont les risques d'une guerre informationnelle ?
Nous procédons dans ce dossier à l'analyse de la déstabilisation des entreprises de défense par l'information en structurant le débat autour de la nature et l'origine de chaque risque informationnel identifié.

Partie I – Contextualisation de l'industrie de défense française

Dans un contexte marqué par les interventions extérieures et les attaques terroristes, le secteur de la défense revêt une importance de plus en plus cruciale. Il s'agit d'une industrie dont la place dans l'économie tout comme la géopolitique est centrale.

A. Structure et acteurs de l'industrie de défense

Une stratégie de fusion-acquisition a été menée aux États-Unis et en Europe entre les années 1990 et 2000. En lien avec les efforts de défense, ces opérations expliquent qu'aujourd'hui les principaux maîtres d'œuvre mondiaux de la défense soient américains et européens. Les maîtres d'œuvre américains (Lockheed-Martin, la division militaire de Boeing, Northrop Grumman, Raytheon et General Dynamics) dominent ainsi le classement mondial des entreprises de défense. À eux seuls, ils représentent 35% du total des ventes d'armes du « top 100 », avec un chiffre d'affaires cumulé de 148 milliards de dollars en 2018[4].

Parmi les huit principaux maîtres d'œuvre industriels opérant en France, seuls Airbus, Thales et Safran sont présents dans le « top 20 » mondial[5]. Cependant, les ventes d'armes combinées des huit entreprises françaises figurant dans le « Top 100 » sont les deuxièmes plus importantes d'Europe, atteignant 23,2 milliards de dollars. Cette prédominance française est due à une augmentation de 30 % des ventes de Dassault Aviation, soutenant par conséquent l'activité de Thales et de Safran[6].
Les principaux maîtres d'œuvre de défense résidant en France ainsi que leur domaine d'activité sont listés ci-dessous :

- **Airbus** : aviation civile et militaire, hélicoptères civils et militaires, systèmes de drones, spatial civil et militaire, électronique de défense, cybersécurité
- **Dassault Aviation** : aviation d'affaires, avions de combat, systèmes sans pilote, avions de patrouille et de surveillance maritime, activités pyrotechniques et spatiales
- **Naval Group** : navires de surface, sous-marins, armes sous-marines, systèmes de combat, systèmes de conduite, intégration navale de drones, MCO et services associés pour bases navales, énergies marines et nucléaire civil
- **MBDA** : système sol-air, missile air-air, munitions guidées, missiles de croisière, missile antinavire, missile antichar
- **Nexter** : véhicules blindés à roues ou chenillés, systèmes d'armes, artillerie et munitions, équipements mécaniques et hydrauliques, équipements électroniques, robots aéroterrestres, équipements d'optique et de vision protégée pour véhicules blindés, protection NRBC, simulation et entraînement

[4] Laurent LAGNEAU, ''L'industrie française de l'armement fait mieux que résister face au rouleau compresseur américain'', *Opex360*, 2019.
[5] SIPRI *Military Expenditure database* 2019
[6] ''Les dépenses militaires mondiales enregistrent la plus forte augmentation annuelle depuis une décennie atteignant 1 917 milliards de dollars en 2019'', *Observatoire des Armements*, 2020.

- **Arquus** : véhicules blindés à roues, véhicules tactiques et logistiques, chaîne de propulsion pour blindés, systèmes d'armes (tourelles téléopérées), MCO et modernisation
- **Safran** : motoriste, systémier-équipementier, propulsion aéronautique, spatiale et missile, systèmes et équipements aéronautiques, optronique, avionique, navigation, électronique et logiciels critiques, systèmes de drones Sécurité (identification, sécurisation, détection)
- **Thales** : systèmes et équipements aéronautiques, senseurs et communications, systèmes d'armes et de munitions, entraînement et simulation, spatial

Les maîtres d'œuvre français présentent plusieurs caractéristiques. D'abord, si des groupes comme Naval Group, MBDA, Nexter et Arquus exercent exclusivement leur activité dans le domaine militaire, d'autres ont une activité duale et produisent des biens et des services destinés tant aux marchés militaires que civils. Ainsi, Airbus ne réalise que 18 % de son chiffre d'affaires dans la défense, compte tenu de la part des ventes d'avions civils. Dassault Aviation est lui aussi dual, mais renforce la croissance de son chiffre grâce à la vente des Rafale[7] (7,3 milliards d'euros, soit une augmentation de 44% par rapport à 2018).
Ensuite, les segments de la production militaire nationale sont dominés par un maître d'œuvre de référence : l'armement terrestre par Nexter et RTD, l'aéronautique par Airbus Group et Dassault Aviation, l'électronique par Thales, la motorisation par Safran, les missiles par MBDA.

B. Des interactions fortes entre États et industriels

1. À l'échelle internationale

Les ventes d'armes restent l'expression privilégiée des ambitions géopolitiques. L'acquisition de matériel de guerre relève en effet de la politique, dans la mesure où elle influe directement sur la qualité des relations bilatérales entretenues avec les principaux pays exportateurs. Ces acquisitions constituent pour la France, qui propose une gamme complète de systèmes de défense à l'export[8], une opportunité de créer ou de consolider des partenariats sur le long terme.
Les États, en tant que responsables du contrôle des transferts d'armements, utilisent en effet leurs exportations comme vecteur de politique extérieure. Le concept de diplomatie de défense témoigne de l'ambition d'utiliser les dépenses militaires pour contribuer à un climat de confiance et à une convergence des intérêts à l'échelle globale.

Les États sont également des acteurs industriels : les choix politiques de posture de défense et de degré de volonté d'autonomie stratégique dimensionnent l'effort de développement de leur base industrielle et technologique ainsi que l'effort de financement de la R&D indispensable à ce secteur de haute technologie.
C'est le cas par exemple de l'Australie, dont le contrat avec Naval Group portant sur 12 sous-marins représente le plus gros budget jamais alloué à un programme de défense. L'objectif

[7] Michel CARIBOL, ''Dassault Aviation a volé vers un « record absolu » d'activité en 2019'', *La Tribune*.
[8] Tant aéronautique, que naval et terrestre.

est d'acquérir les sous-marins les plus performants de la région Asie Pacifique pour faire valoir sa souveraineté sous-marine grâce aux transferts technologiques.

2. À l'échelle nationale

L'État français est un actionnaire investi au sein des groupes de défense[9]. Ces placements stratégiques lui permettent d'être inclus dans les décisions du secteur. De plus, certaines dispositions permettent renforcer son contrôle des entreprises telles que : le droit de vote double, les *golden share* (droit de veto dans les conseils d'administration), ainsi que la protection des actifs. Outre son rôle d'actionnaire, l'État est un client incontournable pour l'armement français. Les financements publics représentent 70% du chiffre d'affaires de l'industrie de défense française[10].

Par ailleurs, l'État français dispose de deux leviers de contrôle : la réglementation et les financements. En effet, du fait du caractère hautement stratégique de ces industries, l'État a adopté un ensemble de textes visant à protéger les industries de défense des ingérences[11], ainsi qu'un ensemble de restrictions[12] contraignantes pour les exportations d'armements français. De même, l'État soutient financièrement les industries de défense à travers des dispositifs tels que le Fonds de restructuration de la Défense (FRED) ainsi que la Banque publique d'investissement BPI-France (et de sa filiale Sofired pour le soutien aux petites et moyennes entreprises de l'armement) ou encore Delta Defence[13].

C. Des exportations à l'international essentielles

L'industrie de défense française apparaît très bien intégrée au marché mondial de l'armement : la France a représenté 7,9 % des exportations de missiles, avions de chasse et navires de guerre de 2015 à 2019, contre 4,8% de 2010 à 2014. Avec une augmentation des ventes d'armes de 72%, elle occupe dorénavant la troisième place du marché mondial des ventes d'armement, alors qu'elle était cinquième lors des cinq années précédentes[14].

1. Principaux pays clients de l'industrie de défense française

Les exportations d'armement français ont effectivement le vent en poupe. Les premiers destinataires, en termes de livraison, sont le Qatar, l'Union européenne (Belgique et Espagne) et l'Arabie saoudite, selon un rapport du ministère français des Armées au Parlement[15].
Le Proche et le Moyen-Orient représentent la première région d'exportation de la France, avec un peu plus de 50% des prises de commandes (seuls les contrats signés et entrés en vigueur sont pris en compte)[16].

[9] Ferghane AZIHARI, ''L'industrie de l'armement sclérosée par l'État actionnaire'', *Les Echos*, 14/09/2018.
[10] Annuaire statistique de la défense - Édition 2017
[11] Décret de 2014 publié au moment des négociations entre Alstom et General Electric.
[12] Soumises au Code de la Défense.
[13] ''Manurhin : la saga d'un fabricant d'armes français'', *France Inter*, 11/07/2018.
[14] Isabelle CHAPERON, ''La France devient le troisième exportateur mondial d'armement'', *Le Monde*, 09/03/2020.
[15] Rapport 2019 au Parlement sur les exportations d'armement de la France.
[16] ''Défense : envolée des exportations d'armes de la France'', *Capital*, 04/06/2020.

Il est important de noter qu'en France, les livraisons à l'Arabie saoudite et aux Émirats arabes unis sont controversées à la suite de leur implication dans la guerre au Yémen. Depuis 2015, ce conflit a entraîné la mort de dizaines de milliers de civils selon diverses ONG.
En termes de montants, l'Arabie saoudite représente le troisième client de la France avec des prises de commandes atteignant pratiquement un milliard d'euros en 2018. L'Inde est le premier client de la France (grâce à une commande de 36 Rafale), devant l'Arabie saoudite, le Qatar, l'Égypte et le Brésil.

2. Enjeux du manque de coopération à l'échelle européenne

Selon une étude de la Commission européenne, le coût du manque de coordination des industries de l'armement au niveau européen représenterait 26,4 milliards d'euros par an[17]. Cela s'explique par le nombre significatif d'avantages non perçus en termes de compétitivité, de rentabilité, déconcentration des financements de recherche et de soutien à l'activité, ainsi que de réduction des dépenses nationales.

Les industries de défense de l'Union européenne bénéficient d'initiatives intergouvernementales telles que l'OCCAR (Organisation conjointe de coopération en matière d'armement), regroupant l'Allemagne, la France, l'Italie, le Royaume-Uni, la Belgique et l'Espagne. Pour autant, ces coopérations entre États ont un coût corrélé au nombre de participants. De ce fait, les dépassements budgétaires atteignent 60 à 80% pour les programmes bilatéraux et jusqu'à 100% pour les programmes quadrilatéraux. La priorité semble être à la préservation de la souveraineté nationale : il s'agirait de réserver les marchés aux entreprises domestiques. C'est le cas notamment du rapport de force entre les industriels navals européens : très dépendants des exportations, la concurrence est acharnée entre Naval Group, BAE Systems au Royaume-Uni, Navantia en Espagne, TKMS en Allemagne, Damen aux Pays-Bas ou encore Kockums en Suède. À titre d'exemple, 22 concurrents ont ainsi répondu à l'appel d'offres concernant l'achat de 4 corvettes par le Brésil en mars 2019[18].

Les États européens ne semblent donc actuellement pas disposés à aller plus loin dans la construction de géants de l'armement.

3. Enjeux et risques des salons internationaux

Les salons internationaux dédiés à l'armement constituent une vitrine prestigieuse pour les industriels de la Défense. Ils représentent une opportunité particulière de présenter les produits, notamment à travers la démonstration de matériels. Il s'agit également de pouvoir échanger avec des délégations étatiques venues du monde entier. En France, de nombreux salons internationaux sont organisés, tels que le Salon de l'Aéronautique et de l'Espace du Bourget, ou encore Eurosatory pour l'armement terrestre, Euronaval pour les équipements navals et Milipol pour la sécurité intérieure. Ces salons constituent donc un vecteur de rayonnement international de l'offre française sur la scène internationale.

[17] Rapport 'La coopération européenne en matière d'armement : un renforcement nécessaire, soumis à des conditions exigeantes'', *Cour des comptes*, 04/2018.
[18] ''Défense : un « Airbus du naval » indispensable pour résister à la Chine, la Russie et la Corée ?'', *Capital*, 04/02/2020.

Pour autant, ces salons peuvent également se transformer en terrain d'affrontement, entre espionnage et contre-ingérence. « *En économie, nous n'avons pas d'amis (…) Nous pouvons seulement avoir des intérêts qui s'alignent avec d'autres, parfois*. [19] » Les propos d'Éric Bucquet, à la tête de la Direction du renseignement et de la sécurité de la Défense (DRSD), soulignent un élément clé dans la lecture des rapports de force à l'œuvre dans le secteur de l'armement.

L'espionnage industriel apparaît comme un phénomène courant durant ces évènements, à travers des actions menées par la Chine ou la Russie[20], mais également par des pays membres de l'Union européenne. Ces actions se traduisent par des tentatives, réussies ou ratées, de vol de secrets industriels, ou de données économiques. Il peut également s'agir d'intercepter des données personnelles afin de mener des attaques d'hameçonnage sur des personnes clés au sein d'entreprises ciblées.

Pour les industriels français, les salons internationaux représentent donc un enjeu de taille dans la gestion du risque informationnel : il s'agit de trouver l'équilibre entre la protection des informations et le besoin de promotion des produits, pour la plupart extrêmement sensibles.

D. Une industrie hautement stratégique pour la France

Certes, le chiffre d'affaires (15 milliards d'euros par an) de l'industrie de défense française apparaît largement inférieur à celui d'autres secteurs, notamment celui de l'agroalimentaire et de l'automobile (respectivement 170 et 104 milliards d'euros).
Pourtant, la législation de l'OMC et de l'Union européenne ne soumet pas l'armement aux mêmes règles que d'autres secteurs économiques.

L'État peut ainsi protéger et stimuler sa base industrielle de défense selon ses propres intérêts. En France, cette protection est vitale compte tenu des 296 000 emplois directs et indirects que le secteur de la défense représente : en 2013, 15 des 50 premières usines industrielles de France étaient des entreprises de l'armement.
Cette concentration industrielle à l'échelle nationale est dépassée uniquement par le secteur automobile, qui compte 17 usines.
Il s'agit donc, pour l'État français, de préserver une industrie vitale en s'affranchissant des règles d'intervention publique conventionnelles.
Selon le Livre blanc sur la Défense et la Sécurité nationale de 2008, 60% de la recherche financée par la Défense a des retombées dans le secteur civil, et 20% en sens inverse.

L'État subventionne 37% des dépenses du secteur de l'armement en Recherche et Développement (R&D). Ces subventions sont trois fois plus élevées que pour tout autre type d'entreprise bénéficiaire de subventions publiques pour la recherche. À titre d'exemple, en

[19] Guerric PONCET, ''Le Salon du Bourget est-il un nid d'espions ?'', *Le Point*, 18/06/2019.
[20] Antoine IZAMBARD, ''Espionnage : quand la Chine déployait ses grandes oreilles au salon Milipol'', *Challenges*, 22/11/2019.

2010, le Crédit d'impôt recherche a dédié 2,3 des 5,2 milliards d'euros à l'industrie de défense[21].

Néanmoins, ce caractère privilégié des entreprises de défense peut également mener à des dérives. En effet, dans une commande de matériel de guerre, les écarts de coûts peuvent être fréquents (dans 87,5% des cas) et représentent en moyenne 10% du prix initial. Les pouvoirs publics acceptent très souvent ces complications du fait de la nature particulière des innovations à usage militaire, qui doivent contrecarrer des technologies ennemies, quel que soit le coût à payer.
Les industries de défense peuvent ainsi tirer parti de leur statut d'industries stratégiques.

[21] Vincent SATGÉ, ''Note de lecture : L'industrie française de défense'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 01/2016.

Partie II – Méthodologie d'identification et d'évaluation des risques informationnels

Les risques informationnels identifiés ci-dessous ont été répartis dans quatre catégories : juridique, humaine, réputationnelle et économique. Ces catégories ont été choisies pour souligner l'origine du risque informationnel (un employé, une réglementation, une sanction, un détournement, une fraude…). La cartographie des risques permet d'appréhender l'ensemble des facteurs susceptibles d'affecter les activités, la performance ou l'image d'une entreprise de défense.

Juridique
Contentieux/Assignation en justice
ITARisation Technologies/Produits
Audits de conformité par des organismes étrangers
Juridicisation à outrance (AFA)
Intégration d'une nouvelle société après fusion/acquisition

Humain
Mauvaise culture du risque
Mauvaise communication
Mauvais management
Employé malveillant ou vengeur (divulgation, sabotage, espionnage)
Manque de sensibilisation
Système informatique obsolète
Attaque Cyber
Supply Chain (sous-traitants)
Lançeurs d'alerte

Réputationnel
Dépendance d'ordre Politique
Mise en cause médiatique
Fraude interne (contournement des procédures de conformité)
Dégradation de la confiance envers l'image de marque
Détournement d'usage
Défaillance dans l'appréciation culturelle
Sûreté des collaborateurs à l'international
Opinion publique (risque interne)
Défaillance rémunération des intermédiaires commerciaux

Économique
Déséquilibre stratégique sur un projet en Joint Venture
Rupture de contrat
Perte de licence d'exportation
Embargo
Échanges en Dollar
Sanctions
Renversement d'alliance
Représailles politiques/diplomatiques
Blacklistage

A. Cartographie des risques

Le modèle de cartographie suivant a été choisi, car il permet de mettre en avant le niveau de maîtrise de chaque risque, et ainsi de mettre en valeur certaines vulnérabilités. L'échelle d'évaluation de l'impact est basée sur quatre catégories d'impact : financier, humain, clients/partenaires, éthique/réputation, savoir-faire/production. Pour évaluer nos risques, nous avons défini l'impact maximal pour chacune de ces catégories :

- **Impact image/éthique :** atteinte grave et durable dans les médias internationaux
- **Impact clients/partenaires** : insatisfaction grave et durable du client ou du partenaire
- **Impact savoir-faire/production** : perte définitive et importante de données stratégiques
- **Impact financier** : tout aléa entraînant une perte de plus de 200 millions d'euros
- **Impact humain** : tout accident entraînant la mort, suffisamment important pour attirer l'attention des médias

NB : Le code de chaque risque fait référence à la catégorie à laquelle il appartient. **J** : Juridique, **H** : Humain, **E** : Économique, **R** : Réputationnel

Le niveau de maîtrise est illustré par un code couleur :

- Rouge : Bas
- Rose : Partiel
- Bleu : Élevé


Impact
Probabilité
CATASTROPHE
CRITIQUE
SIGNIFICATIF
LIMITE
BAS
TRES BASSE
BASSE
MOYENNE
ELEVEE
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
J2 ITARisation Technologies/Produits
J4 Juridicisation à outrance (AFA)
H4 Manque de sensibilisation
H8 Supply Chain (sous-traitants)
H5 Système informatique obsolète
H7 Attaque Cyber
E5 Echanges en dollar
E8 Représailles politiques/diplomatiques
H3 Employé malveillant ou vengeur (divulgation, sabotage, espionnage)
H9 Attaque Cyber
R11 Sûreté des collaborateurs à l'international
J6 Intégration d'une nouvelle société après fusion/acquisition
E2 Rupture de contrat
R3 Fraudes internes (contournement de procédures de conformité)
R4 Détournement d'usage
E6 Sanctions
R2 Mise en cause médiatique
J3 Audits de conformité par des organismes étrangers
H6 Lanceurs d'alerte
J1 Contentieux / Assignation en justice
E4 Embargo
E7 Renversement d'alliance
H10 Manque de management du personnel
E1 Déséquilibre stratégique sur un projet en Joint Venture
R5 Défaillance rémunération des intermédiaires commerciaux
R8 Dégradation de la confiance envers l'image de marque
E3 Perte de licence d'exportation
E9 Blacklistage
R7 Dépendance d'ordre Politique
R10 Opinion publique, risque interne
R1 Compliance/Ethique des affaires
H1 Mauvaise culture du Risque
H2 Mauvaise communication
R9 Défaillance dans l'appréciation culturelle

B. Principaux scénarios redoutés

L'identification des principaux scénarios redoutés permet de quantifier la probabilité d'occurrence des risques identifiés ci-dessus.

- **Interception et divulgation d'informations stratégiques aux médias** : en 2011, Naval Group a été victime d'une fuite massive de données concernant des sous-marins conçus pour l'Inde. 22 000 pages concernant les capacités secrètes de combat de six sous-marins Scorpène ont été divulguées par un ancien employé vengeur. En août 2016, en pleine négociation de contrat (sous-marins classe *Attack*) entre Paris et Canberra, le journal *The Australian* décide de publier les informations qui lui sont parvenues. Certains manuels techniques, ainsi que les modèles des antennes du Scorpène, en passant par les informations sur les capacités en termes de vitesse et de furtivité ont ainsi été révélés. Cette publication suscite un problème stratégique non seulement pour l'Inde, mais également pour la Malaisie et le Chili, tous trois utilisateurs du sous-marin. Quel était l'intérêt, pour l'Australie, de mettre à mal la réputation de son principal partenaire pour les 50 prochaines années ? *The Australian* a déclaré que *« les avantages des nouveaux sous-marins (australiens) seraient sérieusement compromis si des données sur leurs capacités fuyaient de la même manière que pour le Scorpène »*[22].

- **Interruption ou refus de contrat en représailles diplomatiques** : dans le contexte de la mise en examen du président du PSG, le Qatar menace d'annuler un contrat d'armement avec Nexter. En mai 2018, Nasser Al-Khelaïfi, actuel président du PSG d'origine qatarienne, a en effet été mis en examen pour corruption active. Cette mise en examen est dénoncée par l'émir du Qatar, très proche de Nasser Al-Khelaïfi. En représailles, ce dernier menace aujourd'hui la France d'annuler le contrat de deux milliards de dollars passé avec Nexter, qui porte sur la vente de 490 véhicules blindés de combat d'infanterie (VBCI). Le Qatar a d'ores et déjà lancé une potentielle procédure de remplacement de Nexter. De leur côté, l'américain General Dynamics, l'Italien Oto Melara et le Finlandais Patria sont prêts à répondre à l'appel d'offres. Il s'agit donc d'un dossier très sensible pour la France : l'émir du Qatar remet en cause un mégacontrat d'armement qui avait été signé en 2017 en présence du Président français. De ce fait, Florence Parly, ministre des Armées, a rencontré au Qatar fin novembre l'émir du Qatar, ainsi que le vice-premier ministre et le ministre de la Défense. Il s'agit de défendre les intérêts de la France dans un contrat de taille, à travers une société qui appartient à l'État français[23].

- **Traçabilité des contrats par les États-Unis à travers l'application de la norme ITAR** : l'exportation des produits ou services de l'industrie de défense française estampillés ITAR sont soumis à autorisation des États-Unis. Ce système américain de contrôle des exportations est intrusif : l'approbation et l'octroiement d'une licence d'exportation ITAR suppose l'accès à toutes les informations incluses dans le contrat, qu'il s'agisse du fournisseur, du client final, du montant du contrat et des intermédiaires commerciaux

[22] Léna COROT, ''Le drôle de parcours qui a conduit à la fuite de données sur le Scorpène de DCNS'', *L'Usine Nouvelle*, 29/12/2016.

[23] Michel CABIROL, ''Le Qatar près de renoncer au VBCI de Nexter en raison de la mise en examen du patron du PSG'', *La Tribune*, 26/11/2019.

impliqués. Les États-Unis peuvent donc, selon leurs intérêts, s'opposer à certains contrats. C'est le cas notamment des satellites de type Pléiades de Thales et Airbus vendus aux Émirats arabes unis en 2014. La vente avait été décrochée après cinq années de négociations face au concurrent américain Lookheed Martin[24].

- **Retombées économiques d'une assignation en justice** : fin 2017, la justice américaine a ouvert une enquête pour corruption chez Airbus, à la suite des procédures judiciaires déjà en cours depuis 2015 en France et en Grande-Bretagne. Elle porte sur des centaines de millions d'euros de commissions occultes présumées. Le 20 décembre 2018, les craintes d'une amende de plusieurs milliards de dollars et d'une condamnation par le *Department of Justice* américain (DoJ) font chuter Airbus en Bourse (-4,4 %)[25].

- **Vol de données sur un mégacontrat** : la France a vendu 36 avions de combat Rafale en 2016 à l'Inde. Les premières livraisons du contrat estimé à 8,4 milliards d'euros ont eu lieu en 2019. Ce contrat, déjà entaché par des soupçons de corruption et du trafic d'influence, a été marqué en mai 2019 par un cambriolage dans les locaux de Dassault à Saint-Cloud (Hauts-de-Seine). L'effraction est survenue dans les locaux où se trouvait l'équipe indienne traitant le contrat d'exportation du Rafale. L'image de Dassault a été atteinte sous les yeux de son principal client : le *Hindustan Times* parle d'ailleurs d'une tentative d'espionnage dont l'armée de l'air indienne serait victime et Dassault, potentiellement responsable[26].

C. Cartographie des vulnérabilités

Les vulnérabilités du secteur de la défense peuvent être exploitées par un grand nombre d'agresseurs potentiels : pirates informatiques ayant la volonté de nuire ou simplement de montrer leurs capacités, concurrents, employés vengeurs cherchant un gain financier, voire d'autres États voulant déstabiliser un pionnier français. Certaines attaques peuvent être combinées pour en multiplier l'impact.

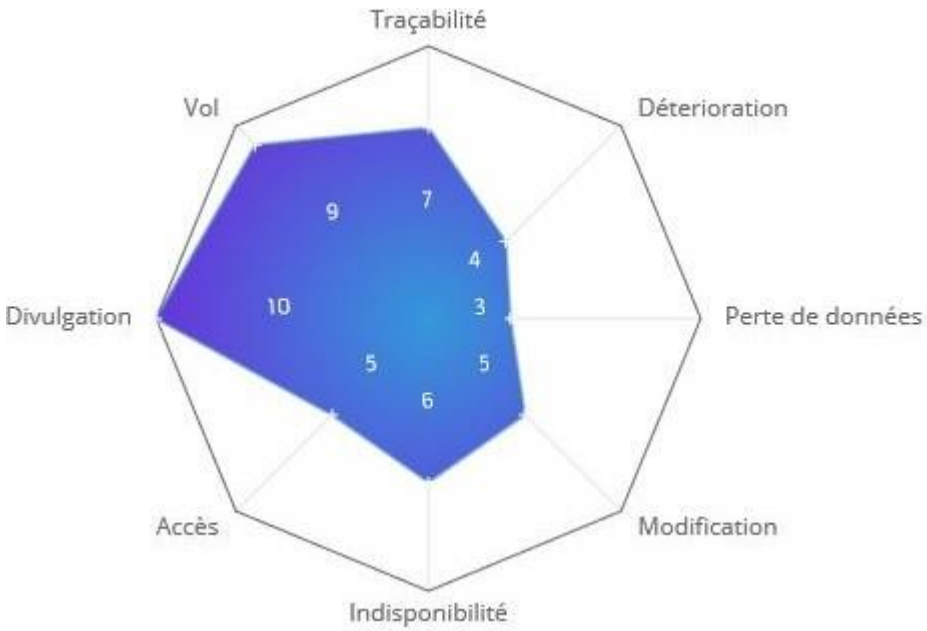
Les évènements redoutés sont accentués par les vulnérabilités suivantes :

- **Sur le plan stratégique** : la concurrence acharnée du secteur doit inciter les hauts décideurs de l'industrie de défense à adopter une stratégie davantage basée sur une grille de lecture des rapports de force. Un contrat d'armement remporté dans un pays ne témoigne d'une alliance avec le client et les partenaires qu'au niveau politique et diplomatique.
- **Sur le plan technique** : une grande difficulté à appliquer une politique rigoureuse, tant au niveau de la cybersécurité, qu'aux procédures de contrôle interne. La contrainte peut engendrer un contournement par facilité.

[24] Nathalie GUIBERT, ''Un contrat de vente de satellites militaires français met au jour les rivalités franco-américaines dans le Golfe'', *Le Monde*, 29/01/2014.
[25] Enrique MOREIRA, Bruno TRÉVIDIC, ''Airbus chute en Bourse après des informations sur une enquête américaine'', *Les Échos*, 20/12/2018.
[26] Simon CHODORGE ''Un cambriolage près de Dassault Aviation à Saint-Cloud éveille des soupçons d'espionnage, en lien avec les Rafale indiens'', *L'Usine Nouvelle*, 23/05/2019.

- **Sur le plan technologique** : une utilisation croissante de systèmes informatiques standards et répandus pour des raisons de coût et d'interopérabilité, dont les vulnérabilités sont bien plus faciles à reconnaître et à exploiter de l'extérieur.
- **Sur le plan commercial** : la réputation de l'entreprise est liée à celle de sa nation d'appartenance et aux décisions de son gouvernement, à sa position sur l'échiquier mondial en termes de stratégie de puissance, de prestige et d'alliances. En outre, l'obtention d'un contrat est soumise au bon vouloir de nombreux acteurs. Par exemple, dans la mesure où les licences d'exportation sont requises très en amont pour certains matériels de guerre, les États-Unis ont la possibilité de s'opposer à un contrat en fonction de leurs intérêts. Il suffit en effet de ne pas accorder de licence d'exportation (selon les normes ITAR[27] et EAR). Par ailleurs, l'impact d'une non-conformité aux réglementations américaine, entraînant sanctions et blacklistage, est trop élevé pour laisser une marge de manœuvre suffisante.

L'analyse des vulnérabilités du secteur de l'armement nous permet de dresser la cartographie ci-dessous. Nous avons procédé en nous posant la question suivante : le secteur est-il plus vulnérable au vol de l'information, à sa divulgation, à son indisponibilité, à sa perte, à sa traçabilité ou bien à sa détérioration ?



Notre analyse de risque souligne que le secteur de l'armement est particulièrement vulnérable à la divulgation, au vol et à la traçabilité de l'information. Nous en concluons dans un premier temps qu'il s'agit de faiblesses liées à une lourde dépendance de l'industrie française aux réglementations internationales et étrangères (notamment américaines). Cette dépendance suppose une distribution de l'information à de nombreuses parties prenantes dans le cadre de l'obtention d'un contrat. De même, ces vulnérabilités sont liées à la mauvaise réputation qui accompagne le commerce des armes : l'augmentation des exportations de matériel de guerre à l'échelle globale s'accompagne nécessairement d'une mise sous les feux des projecteurs et de dénonciations[28].

[27] Voir cas d'étude ''*La norme ITAR et les ventes du Rafale de Dassault-Aviation*'' p.20.

[28] Voir cas d'étude ''*les répercussions de l'affaire Khashoggi sur la réputation de l'industrie de défense française*'' p.34

Nous concluons donc que, dans la guerre de l'information à l'œuvre dans le secteur de l'armement, les entreprises françaises ont une marge de manœuvre réduite : elles ne semblent pas disposées à riposter « par l'information ». Les leviers de défense pour se protéger aussi bien d'une cyberattaque que d'une rumeur propagée doivent donc être renforcés.

D. Enjeux et recommandations pour améliorer la résilience

1. Sécurisation des systèmes d'information

L'activité liée à l'informatique des collaborateurs d'une entreprise de défense doit s'appuyer sur des lignes directrices formalisées pour véhiculer les pratiques à adopter. Sur la base d'un audit, il appartient à la DSI (ou à un prestataire externe) de rédiger la politique de sécurité informatique. Il s'agit de déterminer les secteurs à protéger, les moyens à mettre en œuvre, les procédures à initier ainsi que les responsabilités à définir. Elle doit intégrer l'ensemble du parc informatique, les différents sites du groupe ainsi que l'ensemble du personnel, mais également les fournisseurs et tout l'écosystème des prestataires.
Les vulnérabilités de chaque point d'accès au réseau informatique doivent être recensées et contrôlées : tant au niveau des connexions internet, des bornes Wi-Fi, que des appareils électroniques tels que les ordinateurs, les tablettes ou les smartphones. L'entreprise doit avoir recensé et protégé tous ces points de vulnérabilité. Il s'agit d'une part de limiter le nombre de terminaux (et leur diversité) pour mettre en place des contrôles d'accès efficaces. D'autre part, la DSI doit être en mesure de bloquer l'accès à distance et d'effacer le contenu de ces terminaux, en cas de perte ou de vol.

En outre, la sécurité informatique d'une entreprise de défense exige une démarche globale inscrite dans la durée. Le parc informatique (matériel incluant systèmes d'exploitation, logiciels, paramètres de sécurité, antivirus, pare-feu, etc.) doit être uniformisé à l'échelle de l'entreprise. Les postes informatiques au contenu confidentiel peuvent de plus être coupés du réseau. Il est également important de limiter et de contrôler l'utilisation des solutions cloud qui peuvent présenter des risques. Enfin, le dispositif sécuritaire doit être surveillé et régulièrement mis à jour. En effet, les hackers savent faire preuve d'innovation ; la sécurité des systèmes d'information peut donc rapidement devenir obsolète.

2. Formation et sensibilisation des personnels

La sécurité de l'information repose grandement sur le personnel qui la manipule. Il est donc primordial de dispenser aux personnels des formations adaptées de sensibilisation. Ces mesures devraient s'accompagner de séances obligatoires d'entraînement à la mise en place de Plans de Continuité d'Activité (PCA), d'exercices de crise réguliers, et de la mise en place de fiches réflexes. Il convient en particulier de rappeler aux personnels de faire preuve de sens critique dans l'exploitation ou la transmission d'informations, loin de la confiance aveugle qui fait trop souvent dans nos sociétés hyper connectées.
De plus, une veille régulière permet de corréler avec d'autres sources les informations rendues publiques par une interception et une divulgation.

En outre, lors de salons tels que Le Bourget, les employés doivent limiter l'emport de documents et de matériels sensibles. Les délégations diplomatiques doivent être considérées comme une menace potentielle. En effet, les industriels étant sommés d'accueillir leur client pour des raisons commerciales et parfois politiques, le risque d'espionnage est fréquemment sous-évalué. De même, outre l'exfiltration de données commerciales ou personnelles, le risque de sabotage lors des démonstrations (brouillage de drones notamment) doit être pris

en compte. Cette sensibilisation représente un enjeu de taille pour les industriels, dont la réputation est en jeu autant que l'obtention d'un contrat.

3. Développement d'une culture du risque immatériel

Les risques informationnels identifiés ci-dessus témoignent d'une prise de conscience progressive, mais qui reste à concrétiser dans le monde de l'armement. Ce secteur dispose d'une culture du risque industriel dont les tropismes peuvent représenter des angles morts à plus grande échelle. En effet, afin de rassurer l'actionnariat, les entreprises de défense cotées se doivent de communiquer sur les potentiels risques en raison des multiples dimensions et des incertitudes qu'ils peuvent recéler. Le secteur de l'armement est donc globalement sensibilisé à la gestion stratégique de l'information, en particulier lorsqu'il s'agit de trouver un équilibre entre la protection de l'information sensible et l'obligation de la rendre publique. Pour autant, cette stratégie d'identification des risques et la communication qui en découle sont basées sur une lecture des impacts financiers à court et moyen terme. L'attention semble portée sur les investisseurs et le potentiel manque à gagner[29]. Or, bien que les effets d'une stratégie basée sur la gestion de la réputation ne soient pas calculables à court terme, il ne faut pas oublier qu'une image de marque se construit sur la durée et sera perçue différemment par les diverses parties prenantes.

4. Développement de « l'ITAR-*free* »

L'ITAR-*free* est une stratégie de gestion de la norme ITAR développée par l'industrie de défense. Elle vise à réduire la dépendance de l'armement français aux réglementations américaines[30]. Cette stratégie s'opère à deux niveaux. À court terme premièrement, il s'agit de véhiculer les bonnes pratiques à adopter : on parle véritablement « d'hygiène » de traitement d'informations et de composants ITAR. Cette norme impose en effet aux industriels des contraintes en termes de traçabilité : une entreprise d'armement doit pouvoir à tout moment démontrer le référencement exact des informations ou produits ITARisés.
Une sensibilisation efficace des personnels passe par une responsabilisation des différentes directions impliquées. La gestion du risque ITAR ne relève en effet pas de la seule responsabilité de l'*Export Control* et de la *Trade Compliance*. Il incombe également au RSSI, aux Directions des Achats, Techniques, Financières, et aux ressources humaines de contrôler la propagation du risque parmi les produits et technologies au sein de leur entreprise.
Sur le long terme ensuite, la stratégie ITAR-*free* vise à développer de nouveaux programmes avec des composants similaires aux composants ITAR. Ce procédé passe par de nouveaux investissements dans la recherche, le rachat d'entreprises stratégiques et une concentration sur les programmes de coopération européenne. L'ITAR-*free* peut voir le jour et perdurer uniquement si le risque d'ITARisation accidentelle, lié aux multiples cas d'application de la norme ITAR par la réglementation américaine, est maîtrisé.

[29] ''Airbus : le risque judiciaire diminue, l'action bondit'', *Le Revenu*, 28/01/2020.
[30] Michel CABIROL, ''Réglementation ITAR : la France veut réduire sa dépendance aux États-Unis'', *La Tribune*, 07/09/2018.

Partie III – Risques informationnels de nature juridique

Le risque juridique résulte de la conjonction d'une norme juridique et d'un évènement non maîtrisé. « *Cette rencontre entre une norme juridique et un évènement dans un contexte d'incertitude va générer des conséquences susceptibles d'affecter la valeur de l'entreprise* »[31]. L'importance que jouent les États est redondante lorsque l'on observe l'industrie de défense française. Ils régulent et sont clients sur le marché de cette industrie.
Les risques juridiques qui affectent les entreprises de la défense en France sont les risques émanant d'une mauvaise appréhension des lois qui s'appliquent, voire organisent, le développement de leurs activités. L'intelligence juridique est une réponse pour maîtriser ces risques et nécessite une réelle compréhension de l'environnement règlementaire et légal qui encadre l'exportation du matériel de guerre, mais également sa production.
Afin de définir, analyser et cartographier au mieux ces risques, il a été nécessaire de comprendre si le droit français pouvait devenir un outil d'influence pour les entreprises françaises, si son organisation ou son orientation le permettaient et quelles étaient ses faiblesses.

On constate que les entreprises se heurtent particulièrement aux législations étrangères ou internationales, ce qui provoque une situation d'ingérence dans les exportations. La France est ainsi, par le biais de ses entreprises de l'industrie de la défense, soumise à l'application de corpus juridiques étrangers et dépourvue d'une partie de sa souveraineté en la matière.
L'exemple des ventes de Rafales de Dassault-Aviation a montré que la France était soumise, comme d'autres pays, à l'extraterritorialité du droit américain qui s'exporte via l'application et la reconnaissance de la norme ITAR à l'étranger.

A. Le cadre juridique de l'industrie de défense en France

Le cadre juridique français, qui par ses textes et ses acteurs régit l'industrie de défense, s'exporte peu et ne s'impose pas sur la scène internationale. Il n'est pas à l'heure actuelle perçu comme un outil d'influence par les entreprises françaises du fait de son orientation et de son organisation. Il a eu pour but de répondre au besoin de la défense nationale et aux opportunités d'exportation ou de transferts de matériels de guerre. Les risques juridiques pour les entreprises émanent ainsi de ce cadre, mais également des règlementations et textes étrangers par le biais notamment de l'extraterritorialité du droit.

1. Droit et acteurs français

L'État français s'est positionné comme régulateur, mais également comme client de son industrie de défense. Il a, pendant la période post-Guerre froide de 1990 à 2010, fait le choix d'une industrie peu concurrentielle et de la « sobriété stratégique »[32]. Les lois françaises qui encadrent le secteur de l'industrie de défense en France sont le reflet de l'antagonisme

[31] Christophe COLLARD, Christophe ROQUILLY, ''Les risques juridiques et leur cartographie : proposition de méthodologie'', *La Revue des Sciences de Gestion*, vol. 263-264, no. 5, pp. 45-55, 2013.
[32] Jean-Pierre SAULNIER, ''L'industrie de défense sous contraintes'', *Stratégique*, vol. 104, no. 3, pp. 69-84, 2013.

« État/marché » de ce secteur[33], mais également une traduction des lois internationales limitant l'utilisation et la production de matériels de guerre.

Le droit français a ainsi répondu au besoin de la défense nationale dans un premier temps et a plus tard cherché à rattraper son retard concernant les possibilités d'exporter à l'étranger. Il n'a pas eu pour vacation d'être un outil d'influence dans la guerre informationnelle et économique que se livrent les États et les entreprises. Cela est perceptible lorsque l'on observe l'organisation et l'orientation générales du dispositif juridique français.

Le droit français s'exprime au sujet de l'industrie de défense au travers des Livres Blancs et des lois de programmation militaires, du Code de la Défense, mais aussi par le biais de l'attribution d'autorisations et de licences d'exportation, elles-mêmes encadrées par des lois, décrets et arrêtés spécifiques, notamment les Lois n°2011-702 sur les exportations et transferts de matériels de guerre et n°2012-304 relatives au contrôle des armes modernes, ou encore le Décret n°2012-901 portant sur les importations et exportations hors Union européenne et l'Arrêté du 27 juin 2012 définissant la liste des matériels soumis à une autorisation préalable de l'État pour être ensuite exportés ou transférés[34].

Parmi les institutions qui encadrent l'industrie de défense en France, on compte la Commission interministérielle pour l'exportation des matériels de guerre (CIEEMG), le ministère des armées par le biais de multiples organismes comme la Direction Générale de l'Armement (DGA), la Direction Générale des Relations Internationales et de la Stratégie (DGRIS), les Armées par le biais de ses États-majors, et d'autres ministères comme celui de l'Économie et des Finances notamment avec l'intervention de la Direction Générale des Douanes et des Droits Indirects, et celui des Affaires Étrangères. Par ailleurs, les grands groupes de l'armement en France sont également des acteurs dans l'émission et la formulation de normes, dans la mesure où les « relations » entre l'État français et ces grands groupes de l'armement sont « multiples »[35].

Ces textes, institutions et organismes d'État sont autant d'acteurs dans le processus qui a fait de l'industrie de défense française une industrie sujette aux risques juridiques et faiblesses émanant de son propre système, mais également de systèmes juridiques étrangers et internationaux.

2. Droit et acteurs étrangers

Les asymétries de pouvoir au niveau international et les inégalités d'influence dans le domaine du droit qui en découlent recréent un contexte juridique particulier pour l'industrie de défense française et impactent son développement. À titre d'exemple, le *Department of Justice* (DOJ) américain dispose d'une influence inégalée dans le domaine de l'exportation de matériel militaire. Sa stratégie s'articule notamment autour de l'extraterritorialité de l'application de la norme ITAR (cas d'étude 1). De même, depuis quelques années, l'Allemagne a réussi à bloquer l'exportation de produits d'armement français en adoptant une technique

[33] Martial FOUCAULT, Renaud BELLAIS, ''Industrie de défense : un positionnement à trouver'', *CERI*, 2007.
[34] ''Contrôle des exportations de matériels de guerre et assimilés : le dispositif français'', *DGRIS*, 2017.
[35] Claude SERRAFETI, ''L'industrie française de défense'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 2016.

différente : jouer la montre et retarder l'attribution de ses licences au point de désengager le processus d'exportation.

Parmi les institutions supranationales qui encadrent le secteur en France, on trouve l'Organisation des Nations Unies (ONU) par le biais notamment des articles 26 et 51 de sa Charte de 1945, l'Union européenne (UE), le Conseil de l'Union européenne, l'Organisation pour la Sécurité et la Coopération en Europe (OSCE) et l'Organisation du Traité de l'Atlantique Nord (OTAN) ; auxquels s'ajoutent les décisions des Comités à l'origine des régimes multilatéraux de contrôle des exportations comme le Régime de contrôle de la technologie des missiles de 1987.

Ces institutions ont provoqué la signature de conventions, traités, règlements et codes qui s'appliquent aujourd'hui à l'industrie de défense française dans la mesure où ils limitent et encadrent directement ou indirectement la production du secteur.

On note l'existence de 6 conventions majeures[36]. Parmi les plus récentes on compte la *Convention sur l'interdiction de l'emploi, du stockage, de la production et du transfert des mines antipersonnelles et sur leur destruction* de 1997, et la *Convention sur les armes à sous-munitions* de 2008 qui prévoit l'interdiction totale de la production et de l'utilisation d'armes comme les roquettes M26 et les obus OGR français.

D'autres textes font référence, comme les Traités d'interdiction partielle des essais nucléaires de 1963 et de non-prolifération des armes nucléaires (TNP) de 1968, le règlement CE n°3381/94 du Conseil de l'Union européenne de 1994 sur le régime communautaire de contrôle des exportations de biens à doubles usages, le Code de conduite de l'Union européenne de 1998 définissant une position commune sur les exportations d'armement prenant effet en 2008, et enfin le Traité sur le commerce des armes de 2013 sur le contrôle des armes licites et illicites des armements.

B. Risques identifiés

- **Contentieux, assignation en justice** : le procès d'une entreprise de défense peut potentiellement attirer l'attention du DoJ. C'est le cas de Thales en 2019, mis à mal par son ancien agent commercial dans le Golfe, Wamar International, dirigé par Nabil Barakat. Ce dernier semblait chercher à entraîner Thales dans une bataille judiciaire jusqu'aux cours américaines[37].
  Nabil Barakat aurait réclamé plus d'un milliard de dollars, avec une stratégie claire : tenter d'amener le groupe sur le terrain de la lutte anti-corruption du DoJ américain afin de lui infliger des sanctions.

- **ITARisation des technologies/produits** : si un système d'armes contient au moins un composant américain inscrit dans réglementation américaine ITAR, les États-Unis ont le

[36] ''Proposition de loi visant à renforcer le contrôle sur le commerce des armes et relative à la violation des embargos - Session extraordinaire de 2016-2017 n°695'', *Sénat*, 31/07/2017.
[37] ''Thales attaqué par un ex-agent du Golfe'' *Intelligence Online*, 25/02/2019.

pouvoir d'en interdire la vente à l'export à un pays tiers[38]. Or, de nombreuses entreprises de défense françaises intègrent des composants américains dans de nombreux matériels. *"Notre dépendance à l'égard des composants soumis aux règles ITAR est un point critique"* (Antoine Bouvier, PDG de MBDA).

- **Audits de conformité par des organismes étrangers** : il est reproché à Airbus d'avoir eu recours au cabinet américain Hugues Hubbard & Reed. L'antenne parisienne de ce cabinet a été mandatée (probablement entre 2014 et 2015, avant les enquêtes du *Serious Fraud Office* britannique et du Parquet National Français) par Tom Enders pour mener un audit internet sur les pratiques commerciales du groupe[39]. Sachant que tout cabinet d'avocats américain se doit d'informer la justice américaine en cas d'irrégularité chez un client, pourquoi ne pas avoir engagé un cabinet français ou européen ? Hugues Hubbard & Reed est l'un des deux cabinets reconnus par les autorités américaines pour réaliser des audits de compliance dans le cadre de la loi fédérale contre la corruption, le *Foreign Corruption Practice Act* (FCPA). Il existe donc un risque important de fuite de données sensibles concernant le réseau d'Airbus dans son ensemble, ainsi que son savoir-faire.

- **Juridicisation à outrance (AFA)** : pour répondre au défi de la lutte contre la corruption, la France a modernisé en 2016 son cadre législatif à travers la loi Sapin II. Cette loi a permis de faire évoluer significativement le système judiciaire français avec notamment l'instauration d'obligations de prévention de la corruption et du trafic d'influence. Cette modernisation vise à permettre à la France de s'aligner sur les standards juridiques internationaux. Pour autant, les premiers contrôles menés par l'Agence Française Anti-corruption (AFA) soulève au sein des entreprises françaises[40] : ces dernières estiment, selon le Medef, que la mission de contrôle de l'AFA devrait davantage consister « *aider les autorités compétentes et les personnes qui y sont confrontées à prévenir et détecter les faits de corruption* ». En effet, pour certaines entreprises, la mission de contrôle de l'AFA est davantage perçue comme relevant d'une recherche de preuves susceptibles de conduire à d'éventuelles sanctions, dans des domaines parfois totalement étrangers à la corruption et au trafic d'influence.

- **Intégration d'une nouvelle société après fusion/acquisition** : « *trop peu d'entreprises font le nécessaire pour contrer la fraude et la corruption lors de fusions-acquisitions ou d'investissements en private equity. Elles s'occupent de la due diligence sur la fiscalité, les règles antitrust, les aspects juridiques et financiers, la propriété intellectuelle et les autres ressources spécifiques au secteur. Mais ces facteurs ne font pas de différence si la société que vous souhaitez acquérir est corrompue »* (Antonin Lévy, associé responsable de la pratique droit pénal des affaires)[41]. Une étude récente de Hogan Lovells révèle que seules 63 % des entreprises interrogées en France procèdent à des vérifications en la matière

[38] Michel CABIROL, ''Réglementation ITAR : États-Unis, cet ami qui ne veut pas que du bien à la France'', *La Tribune*, 23/04/2018.
[39] Raphaël BLERE, ''Guerre économique et justice internationale – l'affaire Airbus'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 05/2018.
[40] ''Observations du Medef sur la mise en œuvre de la loi Sapin 2 et la lutte contre la corruption en France'', *Mouvement des Entreprises de France – Direction Internationale*, 10/01/2020.
[41] Cécile DESJARDINS, 'Fraude et corruption : les multinationales en risque dans leurs acquisitions'', Les Échos, 13/10/2019.

avant des fusions-acquisitions à haut risque. Loin derrière la Chine, l'Allemagne ou les États-Unis où plus de 85 % des multinationales procèdent aux vérifications nécessaires.

C. Cas d'étude 1 : La norme ITAR et les ventes du Rafale de Dassault-Aviation

La norme ITAR (*International Traffic in Arms Regulations*) est un système d'autorisations comprenant un classement des matériels de guerre qui relève de la stratégie de sécurité nationale des États-Unis. Elle prohibe « *l'exportation, l'importation ou la réexportation de produits ou savoir-faire militaires américains dont la finalité d'usage aurait été détournée* » et est également rétroactive[42].

Cette norme comprend 21 catégories de produits et composants ; et s'applique également à des services[43] et à des données techniques. Elle s'applique également aux savoir-faire et aux formations requis pour la conception et l'utilisation du produit développé.

Les interprétations de cette norme ainsi que sa reconnaissance par d'autres États permet aux États-Unis d'intervenir et de bloquer la vente de matériels d'armement partout dans le monde. On peut dire que cette reconnaissance internationale s'appuie sur la suprématie juridique[44] et globale que les États-Unis ont su construire depuis de nombreuses années[45]. Il est donc ici question de l'extraterritorialité du droit américain, c'est-à-dire l'application du droit américain au-delà de ses frontières[46].

L'application de la norme ITAR est rendue possible par l'action du *Directorate of Defense Trade Controls* (DDTC) qui est un directoire rattaché au *Bureau of Political-Miliatry Affairs* du gouvernement américain[47]. Ce directoire est habilité à mettre en place le processus pénal nécessaire pour vérifier la conformité des utilisations des produits répondants de la norme ITAR. Étant elle-même responsable de l'application du *Arms Export Control Act* (ACEA)[48], la norme ITAR est au cœur des préoccupations du *Department of State* américain et un de ses outils en matière d'influence et de stratégie.

Les implications de cette norme pour les industriels de la défense français trouvent des illustrations explicites dans l'exemple des ventes de Rafale de Dassault-Aviation.
L'entreprise française Dassault-Aviation a développé le programme Rafale à la demande des Armées françaises (Armée de l'Air et Marine nationale). Ce programme avait pour but de remplacer sept types d'avions de combat par un avion dit « omni rôle » pouvant assurer des

[42] Manon LEMERCIER, ''Norme ITAR : l'exposition des technologies françaises aux restrictions américaines'', *Portail de l'IE*, 19/12/2019.
[43] Romain LOUBEYRE, Cédric WELLS, ''ITAR : incidences juridiques et opérationnelles pour les assureurs de risques spatiaux'', *Pratiques juridiques dans l'industrie aéronautique et spatiale*, 2014.
[44] Emmanuel ROSENFELD, Jean VEIL, ''Le droit, vecteur de la puissance américaine'', *Le Monde*, 01/06/2004.
[45] Mathias REIMANN, ''Droit positif et culture juridique : l'américanisation du droit européen par réception'', *Université de Michigan - Archives de Philosophie du Droit*, 2001.
[46] Félix DE BELLO, Ralph MOUGHANIE, ''Une brèche dans l'« impérialisme juridique » américain'', *Le Monde*, 2018.
[47] ''Directorate of Defense Trade Controls'', *U.S. Department of State*, 2020 [En ligne]
[48] ''The International Traffic in Arms Regulations (ITAR)'', *Directorate of Defense Trade Controls*, 2020.

missions variées[49]. L'avion Rafale Marine, qui est entré en service au sein des Armées en 2002, a fait ses preuves lors de nombreuses missions de l'armée française et est aujourd'hui un produit d'exportation pour la France[50]. Le Rafale comprend plusieurs standards : F1, F2 et F3. Le standard F1 est parti en mission en 2004 avec l'opération « *Enduring Freedom* » avec le porte-avion Charles de Gaulle ; et le F2 a quant à lui servi l'Armée de l'Air et la Marine nationale à partir de 2006[51]. Enfin, le F3 est livré aux Armées en 2008 et comprend de nouvelles capacités.

Le succès commercial du Rafale débute en 2015 alors qu'une première commande de 24 avions est effectuée par l'Égypte[52].
C'est en 2018 que la norme ITAR empêche la livraison de 12 rafales supplémentaires, alors équipés de missiles de croisière SCALP[53]. Développés par l'entreprise européenne MBDA, les missiles SCALP comportent un composant répondant de la norme ITAR : une puce électronique. La seule présence de cette puce électronique parmi la liste des composants du missile SCALP va permettre aux États-Unis de bloquer le processus d'exportation vers l'Égypte grâce à l'intervention du DDTC et de son influence.

Cet exemple montre que la norme ITAR est utilisée comme outil d'influence : ici, elle sert à bloquer un processus d'exportation sans qu'aucune procédure pénale de la part des États-Unis ne soit engagée[54]. Seule l'influence des États-Unis va permettre de bloquer les négociations entre les États français et égyptien.

D. Cas d'étude 2 : Intelligence juridique comme levier d'influence

L'intelligence juridique est définie, comme le rappelle Véronique Chapuis-Thuault[55], par le professeur Bertrand Warusfel par « *l'ensemble des techniques et des moyens permettant à un acteur – privé ou public – de connaître l'environnement juridique dont il est tributaire, d'en identifier et d'en anticiper les risques et les opportunités potentielles, (…) pour pouvoir mettre en œuvre les instruments juridiques aptes à réaliser ses objectifs stratégiques* ».

Il s'agit donc de mettre les informations juridiques stratégiques à disposition des décideurs par un processus de veille juridique. Ce travail de veille permet de « *connaître la réglementation applicable à une activité ou à un produit donné » ce qui « peut s'avérer capital pour prendre une décision d'investissement ou se livrer à une évaluation de marché* »[56].

[49] ''Omni rôle dès l'origine'', *Dassault-Aviation*, 2020.
[50] ''Rafale Marine'', *ministère des Armées*, 2015.
[51] ''Historique de la mise en service du Rafale'', *Dassault-Aviation*, 2020.
[52] ''Le Rafale, ce fleuron tricolore au succès commercial tardif '', *Capital*, 08/10/2019.
[53] Jérémie SAINT-JALM, ''Les enjeux de la réglementation ITAR dans le blocage de la vente de missiles SCALP à l'Égypte'', *Infoguerre : Centre de Réflexion sur la Guerre Économique*, 01/11/2018.
[54] Hervé GUYADER, ''Vente de Rafale bloquée : la France subit (encore une fois) la loi américaine'', *Les Echos*, 28/02/2018.
[55] Véronique CHAPUIS-THUAULT, ''L'intelligence juridique ou le droit comme élément stratégique clé'', in *Manuel d'Intelligence Économique*, 3e édition, Christian Harbulot, Paris, PUF, 2019.
[56] Bertrand WARUSFEL, ''L'intelligence juridique : une nouvelle approche pour les praticiens du droit'', *Le Monde du Droit.*

Dès la fin des années 1990, le professeur Bertrand Warusfel entreprend de promouvoir ce concept nouveau qui suit l'idée de l'intelligence du droit. Il parle d'intelligence juridique et encourage donc les entreprises qui s'engagent dans une démarche d'intelligence économique à « *favoriser l'utilisation stratégique du droit* » [57]. Il entend par là que collecter des informations sur l'environnement juridique des entreprises ne suffit pas. Il est également nécessaire de les mettre en relation avec les objectifs stratégiques opérationnels de ces mêmes entreprises. Déjà en 1999, Warusfel définissait l'intelligence juridique comme une « arme », pouvant « *servir de garantie préventive, de moyen de dissuasion ou d'ultime recours en cas d'incident* ».

L'intelligence juridique est alors doublement efficace : elle permet, par l'information qu'elle délivre aux décideurs, de mieux connaître l'environnement juridique et de procéder à des décisions mieux informées ; mais également de mieux définir les objectifs stratégiques de l'entreprise sur le long terme.
On voit donc que dès sa conception, l'intelligence juridique est un outil d'influence.

Dans le cadre de l'industrie française de défense, classée à nouveau par l'État par la Loi de Programmation Militaire 2019-2025 comme faisant partie des opérateurs d'importance vitale (OIV), il est nécessaire que la prise de conscience de l'importance de l'intelligence juridique se fasse à deux niveaux : au niveau des entreprises du secteur, mais également au niveau de l'État lui-même.

L'État français est régulateur et client de cette industrie française de défense. Il est également garant de sa pérennité et pourrait donc chercher à développer une culture offensive du droit au niveau national pour protéger les entreprises du secteur.

De même, les entreprises motivées par une logique lucrative et de résilience pourraient intégrer de manière plus automatique la démarche d'intelligence juridique.

[57] Bertrand WARUSFEL, ''Intelligence économique et pratiques juridiques'', *Revue de l'Intelligence juridique*, 1999.

Partie IV – Risques informationnels d'origine humaine

En matière de sûreté ou de sécurité de l'information, l'homme est à la fois le maillon fort et le maillon faible de toutes les organisations.

A. Risques identifiés

- **Mauvaise culture du risque** : une gestion du risque efficace vise à identifier les incertitudes et apporter des mesures de mitigation. Or, l'initiative innovante est un élément rarement pris en compte dans les plans d'action. Mieux vaudrait ne rien faire que de risquer de mal faire.
  Dans un monde instable et en pleine mutation, une entreprise ne disposant pas d'une bonne culture du risque n'est pas pérenne.
  L'impact du risque de ne rien faire est dorénavant supérieur à celui des incertitudes. Il s'agit d'identifier les changements majeurs à l'œuvre dans l'environnement du secteur de l'armement et d'évaluer la vulnérabilité des entreprises face à ces évolutions : changement climatique, transition énergétique, marchés et puissances émergentes, *Big Data*, actualisation réglementaire, etc.

- **Mauvaise communication interne** : ne mauvaise communication interne engendrerait en effet une baisse de la productivité des salariés estimée à 24 000 euros en moyenne, par employé et par an. De même, les problématiques de communication influent sur le désengagement des salariés qui coûterait au total 460 millions d'euros par an. Un mauvais climat social peut inciter les employés à ne pas faire remonter certaines alertes (attaque cyber, compromission de données, vol de matériel professionnel…)[58].

- **Erreur professionnelle** : il s'agit d'une négligence professionnelle résultant davantage d'une erreur involontaire de la part de l'employé que de malveillance.
  Par mégarde ou par ignorance, ce dernier peut par exemple permettre à un hacker de pénétrer le système informatique de l'entreprise. Selon une étude[59] conduite par Atomic Research en 2017, plus d'un tiers des sondés indique avoir été « *précédemment impliqué » dans une compromission de données* ». Ces chiffres soulignent un manque de conscience de la menace : 42 % affirment que leur entreprise est à l'abri de la menace interne, alors que 30% indiquent qu'ils n'en sont pas certains[60].
  De même, près d'un tiers des salariés interrogés ignorent l'impact d'une compromission de données ; 26 % d'entre eux assurent ne pas connaître le risque que peut présenter le fait de partager des identifiants informatiques professionnels.

[58] Emma SEURET, ''Une mauvaise communication fait plus de dégâts que l'on ne croit'', *Les Echos*, 20/09/2011.
[59] Le cabinet a interrogé un échantillon représentatif de plus de 4000 salariés (à temps plein ou partiel), également répartis entre l'Allemagne, la France, l'Italie et Royaume-Uni.
[60] Valéry MARCHIVE, ''Menace interne : un vrai manque de sensibilisation, mais aussi un réel risque de malveillance'', *LeMag IT*, 03/04/2017.

- **Employé malveillant/employé vengeur** : les conséquences d'un acte malveillant interne sont souvent plus difficiles à évaluer que pour un acte malveillant externe. L'employé malveillant est plus insidieux, plus discret : son action s'opère à travers de petites touches successives (vol « à la sauvette » de petites quantités). Le collaborateur dispose du temps nécessaire pour identifier les failles, les modes de contrôles, ainsi que l'organisation de la sécurité. Dans une autre mesure, son passage à l'acte peut se justifier par un manque de sensibilisation quant aux répercussions. Les notions d'employé malveillant et d'employé vengeur diffèrent : très populaire après la crise de 2008, l'employé vengeur se différencie de l'employé malveillant à travers l'effet final recherché. L'employé malveillant a un but financier alors que l'employé vengeur a pour motivation de se faire justice lui-même en dénonçant les pratiques de son entreprise.

- **Manque de sensibilisation** : les entreprises de défense doivent s'assurer qu'elles donnent à leurs équipes une chance de comprendre et de prévenir les problèmes liés aux risques informationnels. Or, 47 % des salariés interrogés par le cabinet Atomic Research en 2017 indiquent n'avoir jamais reçu de formation à la protection des données, par exemple. De plus, 27 % d'entre eux estiment que leur entreprise manque de règles de sécurité pour prévenir la perte de données, ou échoue à les faire appliquer.

- **Manque de management du personnel** : une défaillance dans la stratégie de management peut aggraver les risques professionnels tels que le syndrome d'épuisement professionnel (*burnout*), cumulé aux facteurs de risques psychosociaux d'origine professionnelle (RPS). La prévention de ce risque relève de la responsabilité de l'entreprise. Il lui incombe de veiller à ce qu'un épuisement du personnel ne mène pas à des représailles malveillantes.

- **Système informatique obsolète** : l'utilisation de systèmes d'exploitation et de logiciels obsolètes constitue un risque pour la sécurité informatique d'une entreprise de défense. Les failles de sécurité des programmes trop anciens peuvent en effet être facilement exploitées par les cybercriminels[61]. De nombreux logiciels obsolètes ou de vieux systèmes d'exploitation sont encore utilisés au sein des entreprises de défense, comme Windows7. Or, au printemps 2017, le ransomware *WannaCry* a exploité une faille de sécurité de l'OS Windows7 pour infecter des millions de machines à travers le monde.

- **Attaque cyber** : « *dans la complexité des serveurs des entreprises, la force du pirate est de trouver toujours l'aiguille dans une botte de foin. Il a une acuité visuelle qui lui permet de repérer la vulnérabilité d'un système* »[62]. En cela, nous pouvons affirmer que les attaquants ont toujours une longueur d'avance sur l'entreprise. La sécurisation des systèmes informatiques ne peut pas être assurée par la seule sophistication technologique : cela ne prévient pas les attaques cyber. Qui plus est, un tiers des accidents de sécurité proviennent de l'intérieur de l'entreprise, perpétré par un collaborateur ou un employé.

[61] ''Ne laissez pas l'obsolescence altérer dangereusement votre informatique'', *Les Echos*, 12/03/2018.
[62] Philippe TROUCHAUD, La Cybersécurité au-delà de la technologie : comment mieux gérer ses risques pour mieux investir, Paris, Odile Jacob, 2016.

- **Lanceurs d'alerte** : par l'intermédiaire de la loi Sapin II, l'institution d'une protection légale du lanceur d'alerte porte en elle les germes d'un risque informationnel potentiel pour l'entreprise qui devra le gérer en respectant les nouvelles contraintes imposées par la réglementation [63] . Certains acteurs (employé, sous-traitant) pourraient profiter du dispositif offert par la loi Sapin II, alors qu'ils ne sont pas animés de bonnes intentions envers leur employeur ou l'entreprise avec laquelle ils collaborent. D'autres, plus certainement, qui auraient hésité par le passé, seront désormais plus enclins, en toute bonne foi, à lancer une alerte. Face au risque de réputation et d'image, aggravé par les facteurs de médiatisation inhérents à une telle alerte, il est essentiel, pour une entreprise de l'armement de prendre toutes les dispositions permettant de prévenir ce risque.

- ***Supply Chain* (sous-traitants)** : en 2019, lors du forum international de la cybersécurité (FIC), l'ANSSI a pointé du doigt la vulnérabilité des petites entreprises. Pour attaquer les grands groupes, les pirates informatiques s'attaquent à leur chaine de sous-traitants, dont le manque d'expertise et de moyens en fait des cibles faciles[64].

B. Cas d'étude : Airbus, cible d'une attaque informatique

Dans un contexte de pénurie de ressources, les risques informationnels dans l'industrie de la défense, qu'ils soient humains ou financiers, peuvent porter préjudice à la France. La maîtrise de ces risques s'impose pour chaque entreprise dans ce secteur, afin de préserver le savoir-faire opérationnel et les connaissances du capital humain.
L'humain représente la principale source des risques informationnels. En effet, pour qu'une information devienne un risque pour une entreprise quant à sa diffusion, il faut qu'il y ait un vecteur pour la transmettre et la propager. Les failles humaines se trouvent être à l'origine de nombreuses attaques, informatiques notamment.

Les entreprises de défense françaises ne sont donc pas à l'abri de convoitise et d'opportunisme de la part de certaines puissances, notamment la Chine. Depuis quelques années, ce pays est suspecté, par les services de renseignement français, d'être à l'origine de plusieurs cas d'espionnage, notamment au sein d'entreprises de défense telles qu'Airbus[65].
Différents leviers sont mis à profit par Pékin pour capter des informations stratégiques et ainsi répondre aux objectifs que s'est fixés la Chine de moderniser sa défense afin de devenir un leader incontestable du secteur.
Par conséquent, le risque humain au sein des entreprises et, plus particulièrement celles de l'armement, est un risque à ne pas négliger. Plusieurs catégories d'impacts en découlent, telles que le vol de savoir-faire, l'ingérence économique et les pertes financières. À titre d'exemple, selon une étude d'IBM et de Ponemon, une fuite de données peut coûter aujourd'hui en moyenne 3,74 millions d'euros à une entreprise.[66]

[63] ''Lanceur d'alerte : quels risques pour les entreprises après la directive européenne ?'', *Les Echos*, 16/10/2019.
[64] Hassan MEDDAH, ''Les sous-traitants, le nouveau maillon faible de la chaine de la cybersécurité'', *L'Usine Nouvelle*, 23/01/2019.
[65] ''Airbus ciblé par une série de cyberattaques, la Chine soupçonnée'', *Les Échos*, 26/09/2019.
[66] Philippe ALCOY, ''Un pare-feu humain, première ligne de défense en matière de cybersécurité'', *Silicon*, 27/01/2020.

En janvier 2019, Airbus a révélé avoir été la cible d'une attaque informatique par des hackers. Le groupe est en effet régulièrement attaqué par des pirates informatiques : en 2018, il a subi une série de quatre attaques majeures. De nombreuses informations sensibles, confidentielles et stratégiques ont été dérobées, notamment des documents concernant la motorisation de l'avion militaire A400M, de l'avion civil A3550, ainsi que des documents de certification techniques. Les différentes attaques informatiques que l'avionneur français a subies ont toutes un point commun : elles ont transité par un de ses sous-traitants. Les attaques directes envers les groupes de l'envergure d'Airbus sont en effet de moins en moins fréquentes.

La stratégie des hackers évolue face à cette nouvelle défense en s'attaquant aux sous-traitants du groupe, moins protégés. Selon Cybercover, assureur en cyber-risque, les petites et moyennes entreprises courent le plus grand risque en termes de cyber-attaques : elles sont victimes à 60% d'attaques de logiciels malveillants [67]. De plus, seulement 38% de ces entreprises mettent à jour leurs logiciels de sécurité régulièrement.
Le mode opératoire de ces attaques informatiques suivait un même schéma et exploitait plusieurs risques humains, à la fois externes et internes à l'entreprise.

Le premier risque identifié émanait de la *supply chain* d'Airbus. En effet, les sous-traitants Expleo et Rolls-Royce sont à l'origine des dernières attaques dont le groupe a été victime. Les systèmes de protection n'étaient vraisemblablement pas au même niveau de développement que ceux du grand groupe européen. Les cyberattaquants ont ainsi pu pénétrer le VPN (*Virtual Private Network*) que les sous-traitants partageaient avec Airbus. La menace externe fait donc partie d'un des aspects des risques humains auxquels l'entreprise doit faire face. La sécurité de la *supply chain* des sous-traitants est en effet une des premières failles humaines à laquelle Airbus a été confronté lors de ces attaques informatiques. Le manque de sécurisation et de contrôle à cet égard a été le facteur le plus important dans les pertes informationnelles qu'a subi Airbus.

Le deuxième risque humain identifié émanait d'une menace à la fois externe et interne : le manque de réactivité des employés des sous-traitants quant à la détection de ces différentes attaques informatiques est à souligner. Les hackers, en pénétrant le VPN, ont pu se faire passer pour les sous-traitants en endossant leur identité. En 2016, une étude a révélé que près de 65% des violations de données sont dues aux négligences des employés[68]. Il semblerait donc que le manque de sensibilisation des employés ait également contribué à l'efficacité des attaques informatiques.

Le dernier risque identifiable dans ce cas d'étude est, selon l'AFP, l'espionnage : ces attaques auraient été perpétrées depuis la Chine[69]. La vraisemblance de cette attribution s'explique par les ambitions de Pékin dans certains secteurs stratégiques à l'échelle globale. La Chine cherche en effet à se repositionner sur ces secteurs, en témoigne le plan *Made in China* de 2015. Ce

[67] Marc-Henry BOYDRON, ''Cybersécurité : statistiques que toute PME devrait connaître'', *Cybercover*.
[68] Daniel CODELLA, ''Le facteur humain dans la sécurité informatique : quand le manque de réactivité rime avec vulnérabilité'', *Wrike*, 22/11/2019.
[69] ''Espionnage : Airbus cible de plusieurs cyberattaques, la Chine soupçonnée'', *La Dépêche*, 26/09/2019.

plan élaboré sur dix ans vise à transformer l'Empire du Milieu en puissance mondiale manufacturière d'ici 2049.
Pour parvenir à ces objectifs, Pékin privilégie une politique de coopération entre l'ensemble de la population chinoise et le gouvernement à travers une loi, décrétée en 2017, contraignant citoyens et entreprises à coopérer avec les agences de renseignement. Le cas d'Airbus pourrait donc être lié à des groupes de hackers originaires de Chine. Deux groupes liés au ministère de la sécurité d'État chinois (MSE) sont suspectés : APT 10 et JSSD[70].
Rappelons que le MSE est le service de renseignement chinois le plus important, comptant sur le territoire plus de 2 000 000 agents, ainsi que plus d'une dizaine de milliers d'agents à travers le monde. Cet organe représente un levier très efficace dont la Chine tire profit pour accéder à des informations stratégiques susceptibles de bénéficier à son plan 2025.

[70] Jacques CHEMINAT, ''Attaques sur Airbus, la sécurité des sous-traitants en question'', *Le Monde Informatique*, 26/09/2019.

Partie V – Risques informationnels de nature économique

« *En économie, nous n'avons pas d'amis (…) Nous pouvons seulement avoir des intérêts qui s'alignent avec d'autres, parfois*. » (Éric Bucquet, DRSD)

Les risques informationnels du secteur de la défense peuvent avoir des conséquences importantes d'un point de vue économique. Le budget du ministère des Armées pour l'année 2020 est de 37, 5 milliards d'euros[71] (soit 13,7% du budget total). Les crédits consentis pour la modernisation des capacités de nos armées en font le deuxième poste budgétaire de l'État, derrière l'Éducation nationale. L'effort de défense en 2020 représentera ainsi 1,86% du PIB. Les commandes venant de l'étranger par les industries françaises de défense atteignent 9 milliards d'euros en 2018, une somme supérieure à la moyenne des exportations (6 milliards d'euros)[72]. Avec de grands groupes, mais aussi plus 4 000 TPE/PME, on retrouve 13% des emplois industriels dans le secteur de la défense. Les exportations françaises d'armement sont un secteur très rentable pour la France, qui permet aussi d'endiguer le déficit de sa balance commerciale, avec un important secteur R&D et de très fortes passerelles vers les industries civiles[73].

Du fait de la complexité du monde de l'armement et de sa politisation, le risque informationnel a de très fortes retombées économiques, liées au poids de l'économie de défense. Tout d'abord, une licence d'exportation d'armes ne s'obtient que par dérogation gouvernementale, ce qui accroît l'importance du pouvoir politique sur elle. L'État est aussi actionnaire dans de nombreux groupes tels que Thalès (26% du capital détenu par l'État), Naval Group (62,49 % du capital détenu par l'État) etc.

Ainsi, les liens entre l'État et l'industrie de défense sont très étroits, le risque informationnel pesant sur l'industrie de défense trouve de ce fait souvent sa source dans le politique. L'État, et le monde politique à travers lui est un acteur incontournable. Le cas de la vente des BPC à la Russie nous paraît particulièrement éloquent en la matière.

A. Risques identifiés

- **Déséquilibre stratégique sur un projet en *Joint-Venture*** : deux industriels européens de nationalité différente s'associent pour un modèle de navire/arme/véhicule : quels sont les risques concurrentiels, jusqu'à quel point peut-on pousser la coopération sans risque de perte de savoir-faire ? La décision par exemple, de Giuseppe Bono, le patron de Fincantieri, de nommer début novembre Giuseppe Giordo comme directeur de la branche défense du chantier naval italien a déplu à Paris. En effet, Fincantieri et Naval Group doivent coopérer à l'export via leur coentreprise Naviris. Cependant, Giuseppe Giordo fait craindre aux Français que le groupe italien profite de sa posture stratégique dans le Golfe. Giordo a en effet participé à l'obtention du mégacontrat de vente de 28

[71] Aude BOREL, ''Promesse tenue pour le budget de la défense'', *ministère des Armées*, 30/09/2019.
[72] Rapport au Parlement sur les exportations d'armement de la France, 2019.
[73] La plupart des grands industriels d'armement ont aussi des activités civiles.

avions Eurofighter au Koweït en 2016[74]. En nommant Giordo, le PDG de Fincantieri espère reproduire une telle vente dans le secteur naval. Le chantier italien pourrait donc proposer un contrat pour des corvettes du même type que celles qu'il a déjà vendues au Qatar, dans le cadre d'un contrat intergouvernemental. Signé en 2017, ce contrat avait déjà été dénoncé par la France. De plus, depuis 2018, Giordo est membre du conseil d'administration de la *Saudi Arabian Military Industries* (SAMI), entité en charge de négocier les coentreprises avec les groupes de défense étrangers. Naval Group craint de ce fait un rapprochement entre Fincantieri et la SAMI, qui se ferait au détriment de toute coopération.

- **Rupture de contrat** : beaucoup d'entreprises de défense ont recours à des consultants qui les aident, via leurs réseaux locaux, à décrocher des marchés civils et militaires à l'étranger. L'interruption de contrat avec des intermédiaires commerciaux peut mener à des contentieux. C'est le cas d'Airbus, qui, dans le cadre d'une enquête anti-corruption, a soudainement mis fin à une centaine de contrats : des centaines de millions d'euros sont en jeu. Vingt-cinq intermédiaires commerciaux ont donc poursuivi Airbus en justice[75].

- **Perte de licence d'exportation** : l'interruption ou la suspension de licence d'exportation peut impacter le chiffre d'affaires d'une entreprise de défense. La décision de l'Allemagne, en novembre 2018, d'imposer un embargo des ventes et des livraisons d'armes à destination de Ryad (après l'assassinat de Jamal Khashoggi) illustre parfaitement cet exemple. Ce gel avait été prolongé en septembre 2019 pour six mois.
  Lors d'un point presse, Berlin a annoncé le 30 mars 2020 qu'aucune nouvelle demande de licences d'exportation à destination de l'Arabie Saoudite ne sera autorisée jusqu'au 31 décembre 2020[76].

- **Embargo** : l'imposition d'un embargo, du fait de son imprévisibilité, représente un risque économique majeur pour l'industrie de défense. À titre d'exemple, nous pouvons citer le cas de la France qui, le 12 octobre 2019, a décidé de suspendre immédiatement les exportations d'armes vers la Turquie, à la suite de l'offensive lancée par Ankara dans le nord de la Syrie. Le montant des commandes de matériel militaire français par Ankara atteignait 45,1 millions d'euros en 2018[77]. Ce risque souligne la vulnérabilité des ventes d'armement aux aléas géopolitiques.

- **Échanges en dollar** : le dollar est la devise du commerce international par excellence et la monnaie de réserve à l'échelle globale. Il représente 87 % des opérations de change et 50% du commerce dans le monde s'effectuent en dollars. Cette prédominance du dollar s'accompagne d'un risque accru de sanctions. Il existe en effet deux types de sanctions : d'une part celles basées sur un pays donné, qui interdisent de commercer entièrement ou selon une liste de produits. Il existe d'autre part des sanctions basées sur la liste « *Specially*

[74] ''Giuseppe Giordo, le supercommercial de la discorde entre Fincantieri et Naval Group'', *Intelligence Online*, 13/11/2019.
[75] Marie-Béatrice BAUDET, Guy DUTHEIL, Chloé AEBERHARDT, ''Bataille feutrée entre Airbus et ses intermédiaires'' *Le Monde*, 18/12/2017.
[76] Michel CABIROL, ''Exportations d'armes : l'Allemagne approuve de nouvelles livraisons au Moyen Orient'', *La Tribune*, 01/04/2020.
[77] ''Paris suspend ses exportations d'armes vers la Turquie'', *Le Figaro*, 12/10/2019.

Designated Nationals » (SDN). Cette liste inclut toutes les personnes ainsi que tous les organismes avec lesquels les États-Unis interdisent de commercer (sous peine d'être ajouté à la liste). En théorie, ces sanctions ne sont pas reconnues par l'Union européenne, une entreprise française échappe donc à ces sanctions sous réserve qu'elle :
- n'utilise pas le dollar dans la transaction
- n'emploie pas de collaborateurs américains
- ne soit pas implantée sur le territoire américain

Le fait qu'une entreprise échappe à une sanction implique toutefois l'interruption de toute relation avec des partenaires (clients, fournisseurs, intermédiaire commercial) ayant un lien avec les États-Unis[78].

- **Sanctions** : Washington est habilité à interpréter les dispositions de la réglementation relative à l'exportation d'armement, à mener des enquêtes et à engager des poursuites pénales en cas de non-conformité. La loi CAATSA (*Counter America's Adversaries Through Sanctions Act*) est le principal levier dont disposent les États-Unis[79]. À des fins d'efficacité et lorsqu'il l'estime nécessaire, il lui est possible de faire évoluer cette réglementation. Le système américain de contrôle des exportations est rétroactif, extraterritorial et intrusif (dans la mesure où il permet l'accès à toutes les informations incluses dans le contrat, qu'il s'agisse du fournisseur ou du client final). Le danger principal pour les entreprises françaises de l'armement est la sévérité des sanctions applicables. Les amendes qui frappent les sociétés sont en effet extrêmement élevées (plusieurs centaines de millions de dollars).

- **Renversement d'alliance** : depuis peu, l'Arabie Saoudite a changé de posture par rapport à la France. Les industriels français sont en effet de moins en moins consultés par Ryad pour les commandes d'armement. Il y a encore quelques années, Paris représentait la deuxième source d'approvisionnement des navires de guerre pour sa flotte de l'ouest et des systèmes Crotale pour sa défense aérienne courte portée. L'arrivée du prince Mohammed ben Salman a changé la donne. Certains industriels français ne sont même plus conviés à participer aux appels d'offres de Riyad.
  C'est notamment le cas de Naval Group, dont l'offre a été ignorée par le Royaume concernant la commande de deux bâtiments de transport amphibie[80].

- **Représailles politiques ou diplomatiques** : derrière une concurrence acharnée, la crainte de Washington d'une émancipation européenne se manifeste dans le secteur de la défense. Les États-Unis cherchent en effet à limiter les ambitions européennes en matière de politique étrangère et de défense, en dénonçant notamment les risques pour l'OTAN. Ce protectionnisme mettrait l'Union européenne à l'abri de barrières tarifaires et réglementaires, tout en bénéficiant de l'ouverture de l'économie internationale. Plusieurs épisodes de guerre commerciale voient alors s'affronter l'Union européenne et les États-Unis, qui s'infligent des milliards d'euros et de dollars de pénalités en représailles

[78] Pierre-Olivier GOURINCHAS, ''L'hégémonie du dollar risque de durer'', *Le Monde*, 27/09/2019.
[79] Michel CABIROL, ''Sanctions et armement : la realpolitik des États-Unis'', *La Tribune*, 03/10/2018.
[80] Michel CABIROL, ''Armement : la France confrontée à un renversement d'alliance en Arabie Saoudite'', *La Tribune*, 02/03/2020.

économiques et douanières[81].

- **Blacklistage** : une sanction par les États-Unis peut impliquer qu'une entreprise de défense figure sur la liste SDN. Dans ce cas, elle peut être potentiellement exclue de certains appels d'offres. D'autres entreprises peuvent être sanctionnées à leur tour en commerçant avec cette dernière.

B. Cas d'étude : la vente des BPC à la Russie

En 2015, la France décide de ne pas livrer les deux BPC commandés par la Russie à cause de son implication dans la crise de Crimée et dans la guerre du Donbass.

Dès 2014, le Royaume-Uni, l'Allemagne et les États-Unis, alliés de la France, lui demandent de suspendre la livraison des navires. Ce qui peut surprendre, c'est que malgré sa position concernant la livraison des BPC, le Royaume-Uni continue à vendre des armes à la Russie pour un montant de 167 millions d'euros[82]. On constate bien que la perception, et donc l'information, a un rôle crucial dans ce genre de décision. En mars, Laurent Fabius, alors ministre des Affaires Étrangères, déclare qu'en raison de la crise de Crimée, la France "pourra envisager" l'annulation de la vente[83]. Selon Hervé Guillou, PDG de ce qui était alors DCNS (ex Naval Group), les seuls frais de gardiennage et d'assurance coûteraient plus d'un million d'euros par mois[84]. Or, ce n'est qu'en août 2015 que la France informe qu'un accord d'annulation a été conclu avec la Russie. Cette seule hésitation a donc coûté à la France plusieurs millions d'euros.

Il faut ajouter à ces millions d'euros les conséquences financières de l'annulation du contrat. D'après l'accord d'annulation, la France doit rembourser 949,7 millions d'euros[85] à la Russie parmi les fonds avancés, tenant en compte la formation des équipages, évaluée à 56,7 millions d'euros. Thierry Mariani, député LR de l'opposition, a évalué entre 1,5 et 1,6 milliard d'euros le coût de l'annulation en tenant compte de la "*dérussification*" (le retrait des équipements aux normes russes) des navires. *Le Canard enchaîné*, de son côté, estime à 2 milliards d'euros la perte due à l'annulation du contrat[86]. L'hebdomadaire a inclus dans cette estimation le coût du gardiennage, de modification du navire ainsi que l'annulation du contrat de maintenance. Ce dernier devait rapporter 400 millions d'euros aux chantiers de l'Atlantique, de même que l'accord de construction de navires câbliers avec les chantiers russes qui devait rapporter 450 millions ou encore le projet de construction de ravitailleurs franco-russe.

[81] Célia BELIN, Quentin LOPINOT, ''États-Unis - Union européenne : de la compétition à la défiance'', *Vie Publique*, 24/04/2020.
[82] Nicolas VANEL, "Crash du vol MH17 : malgré la crise, les ventes d'armes à la Russie se poursuivent", *LCI*, 23/07/2014.
[83] ''Russie : la France "pourra envisager" d'annuler la vente de Mistral, selon Fabius'', *Le Point,* 18/03/2014.
[84] Guerric PONCET, "L'indécision sur les Mistral coûte un million d'euros par mois à la France" *Le Point*, 28/07/2015.
[85] Laszlo PERELSTEIN, "Mistral : Paris a déjà versé les 949,7 millions d'euros à Moscou", *La Tribune*, 03/09/2015.
[86] ''L'annulation de la vente des Mistral à la Russie, deux fois plus coûteuse que prévu ?'', *FranceTV Info*, 12/08/2015.

Partie VI – Risques réputationnels

Au sein de l'industrie de l'armement, l'image fait partie intégrante de l'appréciation d'une entreprise. La réputation représente 25% de sa valeur [87].

A. Risques identifiés

- **Mise en cause médiatique** : les scandales impliquant une entreprise du secteur de la défense, du fait de l'utilisation faite du matériel de guerre, attirent l'attention des médias. Une telle situation peut conduire un industriel français de l'armement à devoir démontrer publiquement sa bonne foi et sa conformité aux lois américaines ou anglaises quand bien même ses opérations ne semblaient pas l'y soumettre.

- **Dépendance d'ordre politique** : il s'agit d'une dépendance des industriels de défense à la réputation de leur État d'appartenance et de sa politique extérieure. La réputation de l'entreprise est donc indissociable de celle de sa nation d'appartenance et aux décisions de son gouvernement, ainsi qu'à sa position sur l'échiquier mondial en termes de puissance, de prestige et d'alliances.

- **Fraude interne (contournement des procédures de conformité)** : chaque année en France, la fraude interne est à l'origine d'une perte d'au moins 5% du chiffre d'affaires des entreprises, tout secteur d'activité et toute taille confondus. Elle se définit comme une tromperie ou dissimulation illégale et intentionnelle en vue d'obtenir un gain. La fraude interne englobe donc les détournements de biens et de services, les actes de corruption, les comportements non éthiques ainsi que la communication d'informations frauduleuses.

- **Dégradation de la confiance envers l'image de marque** : l'image d'une entreprise peut être entachée à la suite d'une incapacité de cette dernière à tenir ses engagements en termes de respect des délais de livraison, de qualité des produits, de santé financière de l'entreprise. Un mauvais choix stratégique tel que le rachat d'une entreprise ou un partenariat en *joint-venture* sur un équipement peut également en être à l'origine. De même, la révélation d'une faille, telle qu'une fuite d'informations ou encore un piratage informatique peuvent porter atteinte à la réputation d'une entreprise.

- **Détournement d'usage** : les scandales liés au détournement (de l'utilisation ou de la destination finale) du matériel de guerre représentent un risque majeur pour les industriels de défense. C'est le cas des blindés français, dénoncé dans le rapport d'Amnesty International qui démontre, images à l'appui, leur détournement d'usage par l'Égypte dans la répression de la société civile depuis la révolution de 2011[88].

- **Défaillance dans la rémunération des intermédiaires commerciaux** : selon la réglementation internationale, un contrat d'armement doit systématiquement être à durée déterminée. Il peut être renouvelé selon le besoin, mais doit toujours disposer

[87] ''Risque de réputation'', *NovEthic*, 26/02/2020.

[88] Marie VERDIER, ''Des blindés français utilisés pour réprimer les opposants en Égypte'', *La Croix*, 16/10/2018.

d'une date butoir de rémunération. Sans cela, un intermédiaire commercial est susceptible de réclamer ce qui lui est dû, sans possibilité de prouver qu'il a été payé à hauteur de ses prestations. C'est le cas de Thales, impliqué dans l'affaire *Bakarat* (mentionné p.18)

- **Défaillance dans l'appréciation culturelle** : une mauvaise prise en compte des us et coutumes d'un pays donné peut engendrer un affaiblissement de la réputation de l'entreprise auprès d'une communauté d'acheteurs.

- **Opinion publique, risque interne** : atteinte à l'image de marque spontanée ou organisée et malveillante. Il s'agit d'un risque pour l'attractivité de l'entreprise en termes de Ressources Humaines qui peut compromettre le recrutement de nouveaux ingénieurs, ouvriers, ou cadres en remettant en cause leur sentiment d'appartenance.

- **Sûreté des collaborateurs à l'international** : atteinte à la réputation liée à la mise en cause de l'entreprise en cas d'accident, d'assassinat ou d'agression d'un employé. En décembre 2019, la responsabilité de Thales a ainsi été mise en cause dans l'assassinat d'un de ses ingénieurs à Bogota (Colombie)[89]. La mission de l'employé avait d'abord été suspendue pour des raisons de sécurité puis finalement maintenue.

B. Cas d'étude 1 : sous-marins australiens classe Attack, atteinte à l'image de Naval Group

Contexte :

En 2016, Naval Group remporte un appel d'offres pour le renouvellement de la flotte de sous-marins de la marine australienne face à l'allemand TKMS et au consortium japonais Mitsubishi-Kawasaki. Après trois ans de négociation, un nouveau contrat est signé en 2019 fixant les grandes étapes pour le développement d'une base industrielle souveraine et le transfert des technologies qui permettront la construction de 12 sous-marins de classe *Attack* sur le sol australien. Le contrat s'élève à près de 32 milliards d'euros et s'étend sur une période de 50 ans.[90] C'est le plus gros contrat d'armement jamais signé par l'Australie ainsi que le plus gros contrat en valeur jamais remporté par un industriel européen.

Il s'agit pour l'Australie de renforcer ses capacités militaires et son autonomie stratégique dans un contexte de hausse des tensions en Asie de sud-est provoquées par une opposition de plus en plus vive entre les États-Unis, garants de la stabilité régionale depuis la fin de la Seconde Guerre mondiale, et la Chine, qui souhaite s'affirmer comme puissance hégémonique dans la région, notamment sur le plan militaire. Le contrat est donc hautement politique de par la taille des enjeux financiers et géopolitiques.

Déstabilisations informationnelles

[89] Sarah UGOLINI, ''Français tué à Bogota : la famille pointe la responsabilité de Thales'', *RTL*, 05/12/2019.
[90] Lilas-Apollonia FOURNIER, ''Sous-marins : Naval Group signe le contrat du siècle en Australie'', *La Croix*, 11/02/2019.

Quelques mois après la sélection de Naval Group en 2016, le journal *The Australian* publie des fuites de données sur les capacités de combat des sous-marins *Scorpène* conçus pour la marine indienne et dont plusieurs unités ont été achetées par la Malaisie, le Chili et le Brésil.[91] Ces révélations surviennent alors que des cyber attaques ciblant les plans du futur sous-marin australien construit par Naval Group ont été détectées[92].

Bien que les fuites de données ne concernent pas les sous-marins de la classe *Attack*, la crédibilité de Naval Group est mise en question dans la presse. Selon *The Australian,* « *les avantages des nouveaux sous-marins australiens seraient sérieusement compromis si des données sur leurs capacités fuyaient de la même manière que pour le Scorpène* ». En effet, le sous-marin français a été choisi en grande partie pour ses capacités furtives. « *Si l'ennemi connaît les secrets du sous-marin, la partie est perdue* », écrit le journal, dans un article titré « *Les Français savent-ils garder un secret ?* ».[93]

Ces révélations, qui concernent des informations sensibles normalement protégées par l'État français, tombent à point nommé alors que Naval Group vient tout juste de remporter l'appel d'offres australien. On ignore encore les circonstances exactes de la fuite, mais il pourrait tout à fait s'agir d'une manœuvre de déstabilisation orchestrée par une puissance étrangère, ou d'un acte de guerre économique mis en œuvre par des concurrents de Naval Group.[94] Quelles que soient les raisons de la fuite, il s'agit alors d'une actualité embarrassante pour la France et Naval Group, que les détracteurs du programme *Attack* vont exploiter pour détériorer la réputation du constructeur auprès de l'opinion publique australienne.

Il s'agit ici du cinquième risque que nous avons précédemment identifié dans la cartographie des risques réputationnels du secteur de la défense : *Dégradation de la confiance des acheteurs envers l'image de marque*.

En 2017, un groupe de lobbying, *Submarines for Australia*, est fondé par un certain Gary Johnston afin de dénoncer le partenariat franco-australien. C'est la politique du gouvernement australien qui est principalement visée, notamment la décision de ne pas recourir à des sous-marins nucléaires,[95] mais les réputations de Naval Group en tant qu'industriel et de la France en tant que partenaire stratégique sont largement attaquées pour décrédibiliser le programme. L'organisme commandite et publie sept rapports entre septembre 2017 et avril 2020 dont le contenu est constamment à charge vis-à-vis du projet. La principale critique vise la décision politique du gouvernement australien de ne pas utiliser de sous-marins nucléaires. Mais le monopole attribué à Naval Group pour la construction des sous-marins *Attack*, ainsi que les coûts élevés du programme sont régulièrement évoqués

[91] ''DCNS victime d'une fuite massive de données sur son sous-marin Scorpène'', *La Tribune*, 24/08/2016.
[92] Dominique GALLOIS, Caroline TAIX, ''Enquête française sur une fuite massive de données de la DCNS sur le sous-marin Scorpène'', *Le Monde*, 24/08/2016.
[93] Cameron STEWART, ''Submarine documents leak: $50bn down gurgler if French can't keep secret'', *The Australian*, 24/09/2016.
[94] Léna COROT, ''Le drôle de parcours qui a conduit à la fuite de données sur le Scorpène de DNCS'', *L'Usine Nouvelle*, 29/12/2016.
[95] Andrew GREENE, ''French submarine program 'dangerously off track' warns report urging Australia to consider nuclear alternative'', *ABC.net*, 10/03/2020.

pour plaider en faveur d'un arrêt du partenariat. Plusieurs articles sont publiés dans la presse australienne citant ces différents rapports.

Par exemple, on peut notamment lire une synthèse de l'argumentaire mis en avant par le groupe de pression dans l'introduction du rapport publié en mars 2020 : « *En décembre 2019, la marine américaine a commandé neuf sous-marins d'attaque à propulsion nucléaire de classe Virginia pour un prix contractuel de 22 milliards de dollars (soit environ 33 milliards de dollars australiens). Ils seront deux fois plus grands que les sous-marins australiens de la classe Attack, avec une capacité offensive nettement plus puissante et une endurance illimitée. Ils entreront tous en service au cours de cette décennie, le neuvième submersible étant livré en 2029, alors que nous attendrons toujours le premier sous-marin de la classe Attack. Quand j'ai entendu l'annonce de Malcolm Turnbull* (ancien Premier ministre australien) *sur le futur sous-marin, je n'ai littéralement pas pu y croire. À l'époque, les Français ont proposé de convertir leur Barracuda à propulsion nucléaire en un sous-marin à propulsion diesel-électrique (ils reconnaissent maintenant qu'il s'agira d'un nouveau modèle). En d'autres termes, il s'agissait d'affaiblir un sous-marin nucléaire en supprimant toute la base de sa capacité supérieure, puis de faire payer au moins deux fois plus cher un sous-marin beaucoup moins performant. Lorsque le premier de la classe sera livré, il sera probablement obsolète* ».[96]

On constate ici l'apparition d'un nouvel acteur dans l'environnement informationnel de l'entreprise, qui se montre hostile vis-à-vis de Naval Group. Bien organisé, déterminé, connu du pays client et disposant de plusieurs soutiens importants, il peut jouer un rôle déstabilisateur sur l'opinion publique locale et nuire de manière significative aux intérêts de l'entreprise. Les risques identifiés ici sont principalement : le risque 2, *Risque politique*, car c'est la volonté politique à la base du partenariat industriel franco-australien ainsi que le choix de sous-marins non nucléaires qui sont ciblés ; et le risque 5, *Dégradation de la confiance des acheteurs envers l'image de marque*, dans la mesure où la fiabilité de Naval Group et sa capacité à tenir ses engagements sont constamment mises en doute afin de créer un mouvement d'opinion défavorable au programme.

<u>Risques identifiés dans l'étude de cas :</u>

- **Dépendance d'ordre politique** : d'un point de vue culturel et sécuritaire, l'Australie entretient des liens très étroits avec le monde anglo-saxon, notamment avec son partenaire américain, alors que les relations avec la France sont beaucoup moins développées. Naval Group n'est pas un partenaire historique de l'Australie et ne dispose pas d'une base de soutien dans l'opinion publique locale.
  Le contrat signé pour la livraison de 12 sous-marins de classe *Attack* a donné lieu à des critiques ciblant la politique industrielle et de défense du gouvernement australien. Certaines informations ont été instrumentalisées pour porter atteinte à la crédibilité de l'industriel français afin de remettre en question le partenariat franco-australien. La réputation de Naval Group est visée à des fins de contestation des choix politiques du gouvernement local.

[96] Mike YEO, ''Australia's Future Submarine, Do we need a plan B ?'', *Asia-Pacific Defence Reporter*, 10/03/2020.

- **Dégradation de la confiance des acheteurs envers l'image de marque** : à la suite d'erreurs de communication, à l'instrumentalisation des fuites de données sur les sous-marins *Scorpène*, et à la publication de multiples rapports dénonçant les insuffisances de Naval Group, différents acteurs cherchent à répandre l'idée selon laquelle le constructeur français n'est pas un partenaire fiable afin de mobiliser l'opinion publique à son encontre. La réputation de Naval Group est mise en cause à plusieurs reprises.

C. Cas d'étude 2 : les répercussions de l'affaire Khashoggi sur la réputation de l'industrie de défense française

L'assassinat du journaliste Jamal Khashoggi le 2 octobre 2018 a poussé l'Allemagne à suspendre ses ventes d'armes à Riyad. De son côté, Donald Trump a déclaré qu'il ne voulait pas saboter la "*formidable commande*" d'armes en provenance d'Arabie Saoudite. À travers l'Europe, un sentiment de gêne est apparu sur la valeur morale des ventes d'armes à l'Arabie saoudite, alors que le pays prend part à la guerre au Yémen. Ce débat sur l'utilisation de matériel de guerre contre des civils se heurte aux réalités économiques des pays exportateurs. La France, premier pays européen fournisseur d'armement à l'Arabie saoudite, est partagée entre sa volonté de faire pression sur Ryad d'un côté et celle de préserver ses intérêts économiques, militaires et diplomatiques de l'autre. Ce dilemme latent est dénoncé par des ONG : des appels à l'arrêt des ventes d'armes à Ryad ont en effet été lancés en raison des nombreuses victimes civiles provoquées par les bombardements de la coalition menée par Ryad au Yémen. Il est donc reproché à la France d'y contribuer indirectement.

Depuis le début du conflit, des organisations telles qu'Amnesty International, Action, sécurité, éthique républicaines (ASER), l'Action des chrétiens pour l'abolition de la torture (ACAT), *Campaign Against Arms Trade* (CAAT) ou encore *Human Rights Watch*, signalent que les armes utilisées proviennent des États-Unis et de l'Union européenne. L'Arabie saoudite et les Émirats arabes unis sont en effet les clients principaux de la France, du Royaume-Uni, de l'Allemagne, de l'Espagne, ou encore de l'Italie. Des actions en justice, devant la Cour pénale internationale et les tribunaux nationaux ont été entamées par des ONG[97] pour dénoncer la complicité des pays exportateurs.

Selon des notes divulguées de la DRM, les canons Caesar de l'industriel français Nexter pourraient atteindre 436 370 civils yéménites et *« appuient les troupes loyalistes et les forces armées saoudiennes dans leur progression en territoire yéménite »* à des fins pourtant essentiellement défensives. Or, certains médias ont démontré que 35 civils avaient été tués dans des bombardements d'artillerie à portée des Caesar : la distance étant trop élevée pour les canons d'origine chinoise et américaine présents dans la zone[98].

[97] En France —ASER, ACAT, en Belgique — Coordination nationale d'action pour la paix et la démocratie (CNAPD), Ligue des droits de l'homme —, au Royaume-Uni (CAAT), en Italie — *European Center for Constitutional and Human Rights* (ECCHR), *Rete Disarmo* , au Yémen — *Mwatana for Human Rights*, aux Pays-Bas — *Public Interest Litigation Project, Nederlands Juristen Comité voor de Mensenrechten* (PILP-NJCM), PAX, *Stop Wapenhandel.*

[98] Romain MIELCAREK, ''Impuissance ou cynisme face aux ventes d'armes européennes'', *Le Monde Diplomatique*, septembre 2019.

Pour la France, les exportations de matériel de guerre contribuent d'une part à l'équilibre de son industrie de l'armement qui est nécessaire à l'autonomie stratégique de l'équipement des armées françaises. D'autre part, ces ventes à l'international constituent un levier d'influence que Paris peut mettre en œuvre sur ses différents clients. En 2018, l'Arabie saoudite se trouvait être le deuxième client de la France depuis les dix dernières années. Ainsi, renoncer à un tel client signifiait perdre un marché colossal, impactant l'équilibre budgétaire d'entreprises majeures du secteur de l'armement français, et, indirectement, la capacité de la France à équiper ses propres forces.

Pour autant, le fait que la France soit devenue le troisième exportateur mondial de matériel de guerre a été mal perçu par les français. En effet, le grand public semble savoir peu de choses de ce fleuron industriel français, de ses usines, de ses salariés, des régions productrices d'armes et des grandes instances d'État chargées de les vendre.
La place de la France dans le classement mondial des exportations est rapidement associée à l'affaire Khashoggi. À l'échelle nationale, l'activité des industriels de l'armement apparaît soudain sous le feu des projecteurs : « *au sein de l'État, qui arbitre lorsqu'il s'agit de vendre à des régimes suspectés de crimes de guerre ? À quoi la realpolitik nous contraint-elle ? Si les armes sont si cruciales pour l'emploi des Français, si elles participent autant à l'indépendance de notre pays, pourquoi y sont-elles un angle mort du débat public ?* »[99]. Le livre « Mon pays vend des armes » (2019) retrace une enquête menée par la journaliste Anne Poiret sur les ventes d'armes françaises à l'étranger basée sur de nombreux témoignages anonymes. Elle contribue à médiatiser les grands contrats de l'industrie de défense française obtenus en Égypte et en Arabie Saoudite. Or, l'Égypte du maréchal Abdel Fattah Al-Sissi mène une répression violente contre ses opposants et l'Arabie saoudite est engagée dans une guerre au Yémen. La journaliste reproche donc aux industriels du secteur d'être protégés par le prétexte de la lutte contre le terrorisme. Le secteur français de la défense apparaît comme un milieu opaque dans lequel la corruption est tolérée et les frontières entre public et privé, inexistantes.

En outre, le 17 septembre 2019, une campagne médiatique intitulée « *#FrenchArms* » a été lancée par Lighthouse Reports, en coopération avec Arte, Mediapart, RadioFrance et Bellingcat. Cette campagne vise à démontrer que les exportations françaises d'armements contribuent à la violation des droits de l'Homme au Yémen, en Libye, au Cameroun et au Maroc[100]. Le matériel de guerre ciblé est le suivant :
- les corvettes militaires de Naval Group participant au blocus maritime du port d'Al Hodeida au Yémen
- les blindés d'Arquus utilisés par les bataillons d'intervention rapide au Cameroun dans le cadre de la lutte anti-terroriste
- les Rafale de Dassault vendus à l'Égypte qui appuieraient l'offensive égyptienne en Libye.

[99] Anne POIRET, ''Mon pays vend des armes'', Paris, les arènes, 2019.
[100] Julia GALAN, ''Silence, on arme !", #Frencharms: les campagnes contre les ventes d'armes françaises se multiplient'' BFMTV, 23/09/2019.

Conclusion

Le phénomène de guerre informationnelle fait rage dans plusieurs secteurs en France. L'information et sa divulgation sont des leviers de déstabilisation et donc d'influence dans un secteur de l'armement déjà complexe. L'industrie de défense est en effet une industrie particulière à plusieurs égards. Elle figure parmi les industries de pointe, ce qui signifie qu'elle est à l'origine et utilise des techniques et savoir-faire, qui se diffuseront ensuite dans d'autres branches d'activité. La nécessité d'une sécurité absolue implique la mise en œuvre de technologies très élaborées. Il s'agit d'une industrie réclamant un grand nombre d'actifs pour générer un revenu dont les besoins en R&D font appel à du personnel hautement qualifié. C'est également une industrie de production particulière (de la pièce quasiment unitaire à la petite série) pour laquelle les gains d'échelle sont plus difficiles à calculer que pour d'autres industries manufacturières.
Il est important de noter que la France figure en bonne place parmi les grandes nations aéronautiques et spatiales, et qu'elle en fut d'ailleurs une des deux pionnières.

Par ailleurs, ce secteur est, du fait de sa nature régalienne, étroitement lié aux actions et aux demandes de l'État français. Il est régulé, encadré et émulé par des actions gouvernementales. Il s'organise d'une part selon les lois votées par ce même État français aux niveaux national et international. D'autre part, il fait face aux lois offensives d'autres États (notamment les États-Unis) et aux organisations supranationales telles que l'Organisation des Nations Unies.
En ce qui concerne la demande qui fait vivre la production du secteur, elle émane majoritairement de clients bien particuliers : les États eux-mêmes.
Ainsi, du fait des lois qui s'appliquent à lui et des demandes qui segmentent son activité, le secteur français de la défense évolue dans un cadre peu transparent et obscur dont les lignes directrices manquent de clarté. Il est important de noter que les informations qui constituent et organisent ce secteur ne sont pas des informations « blanches ». Elles sont difficiles à trouver et on peut les qualifier de « grises ».
En effet, au niveau national, l'État français répond à son besoin à travers la réglementation, c'est-à-dire qu'il est dans son intérêt de soutenir les actions des entreprises françaises qui le renforcent. Au niveau international, ce qui est permis est moins évident : tout dépend de l'intérêt d'un État à commercer ou à accepter l'exportation de matériel de guerre. Selon ces multiples arbitrages, un contrat sera remis en cause ou non par une ou plusieurs parties prenantes. Les leviers d'attaque et de défense dépendent des informations accessibles aux acteurs en question.

La guerre par l'information n'a donc aucune raison d'épargner le secteur français de l'industrie de défense. Bien au contraire, l'information y joue un rôle crucial, tant pour le développement des produits, que pour leur commercialisation ou leur exportation.

Dans ce contexte, l'industrie française de défense reste soumise à quatre grands risques de nature informationnelle :

- Les risques juridiques ;
- Les risques humains ;
- Les risques économiques ;
- Les risques réputationnels.

Les risques juridiques peuvent paraître plus facilement identifiables, car ils découlent d'un manquement à une loi, mais ils n'en restent pas moins complexes. Il s'agit ici d'être le mieux informé possible sur les processus juridiques qui peuvent entraver la production et l'exportation de produits. Les responsables de la mise en application de ces lois sont les États. Le dialogue nécessaire au bon déroulement des opérations de développement ou d'export s'effectue donc au niveau étatique et non simplement entre entreprises et clients. À ce sujet, l'État français, tout comme ses entreprises du secteur de la défense, reste tributaire de nombreuses réglementations étrangères ou supranationales. L'intelligence juridique est un outil d'influence qui mériterait d'être intégré de façon plus automatique par les entreprises et que l'État devrait veiller à développer et à soutenir. Une autre étape serait de développer une culture plus offensive du droit en France de telle façon que les entreprises françaises, tout comme l'État, puissent s'appuyer sur un dispositif juridique propice à la protection des entreprises et du secteur de façon plus globale.

Les risques humains reposent, comme leur nom l'indique, sur les négligences humaines ou bien sur les intentions malveillantes d'un individu ou de plusieurs individus. De même, une erreur de management ou de communication, ou encore une décision prise basée sur des informations incomplètes ou fausses peuvent déstabiliser une entreprise du secteur de la défense.

Les risques économiques reposent sur la conjonction de plusieurs phénomènes, à la croisée entre le contexte économique du marché dans lequel l'entreprise souhaite investir et la décision de l'entreprise elle-même de développer ou d'exporter, bref, d'entreprendre une ou plusieurs activités sur ce marché. Les risques économiques sont emprunts à une très grande instabilité du fait de la multiplicité des acteurs et des paramètres qui amènent à la décision.

Les risques réputationnels quant à eux, sont sans doute les plus redoutés, car les entreprises de défense sont de plus en plus lourdement sanctionnées pour non-respect de l'éthique des affaires. « *Ce qui était secret ne le reste pas, ce qui était toléré l'est de moins en moins, et respecter le droit ne suffit plus »*[101]. Désormais, les autorités de contrôles étatiques mais également les ONG et les médias disposent d'une volonté de recherche de la faute et de capacités d'investigation à l'échelle globale. En conséquence, l'opinion publique à l'égard du commerce de matériel de guerre se montre aujourd'hui aussi intransigeante qu'une juridiction. Par ailleurs, les parties prenantes sont de plus en plus exigeantes quant à l'intégrité des entreprises de défense (notamment les investisseurs et les donneurs d'ordre). Dans un contexte d'instabilité juridique et géopolitique, une entreprise impliquée dans un scandale est en danger sur trois niveaux : celui des sanctions financières, celui d'accès aux marchés et celui de dégradation durable de son image.

L'élément commun à la gestion de ces quatre risques, au-delà du fait qu'il repose sur l'anticipation des informations produites et divulguées, est l'impossibilité d'être entièrement résilient.
Dans le contexte de guerre informationnelle qui est le sien et qui sévit également au niveau légal, l'industrie de défense française n'est pas dans une posture de riposte. Elle peut par

[101] Jean-Baptiste SIPROUDHIS, ''La compliance, un instrument éthique de prévention des risques'', *Atos*, 25/07/2018.

exemple tenter d'échapper aux réglementations étrangères qui la contraignent, notamment la norme ITAR, en développant des produits « ITAR-*free* ». Cependant, cela reste un défi majeur pour les entreprises françaises de ce secteur qui peinent encore à se libérer de leurs appuis technologiques antérieurement ITARisés.
De plus, à cela s'ajoute la mauvaise culture du risque qu'ont les entreprises du secteur de la défense en France. Ces entreprises ne sont pas encore en capacité de mener une bonne anticipation des risques informationnels.
Le plan d'action par lequel il est nécessaire de répondre à l'existence de ces risques reste donc un point d'attention pour les entreprises du secteur.

Annexes

D. Annexe 1 : Interview Bernard Rey – Thales

Business Development, branche Défense, expert Terre

- Bonjour Monsieur Rey, pouvez-vous vous présenter s'il vous plaît et nous expliquer votre rôle actuel chez Thales ?

Bonjour, je suis ancien officier de l'armée de terre, Saint-cyrien, j'ai servi 31 ans dans l'armée de terre où j'ai occupé plusieurs fonctions opérationnelles. J'ai décidé de quitter l'armée et de rejoindre l'industrie de défense, c'est pourquoi j'ai rejoint Thales en septembre 2019.

- Selon vous, existe-t-il des risques réputationnels spécifiques au secteur de la défense ?

Bien sûr, car c'est un secteur où la concurrence est rude, également car l'industrie de défense est un domaine stratégique pour les États, et qu'en portant atteinte à son industrie de défense, on porte atteinte à ses intérêts directs. Le secteur de la défense développe et fournit les armements qui vont permettre de défendre un pays. Donc en portant atteinte au crédit d'une entreprise sur ses marchés export notamment, on peut mettre en péril l'État d'appartenance.
À l'inverse, le secteur de l'armement participe, à travers ses relations commerciales à l'export, à consolider les alliances et les partenariats diplomatiques entre les pays, ce qui constitue également un enjeu majeur et spécifique à ce secteur. On observe sur certains marchés Proche-Orient, Asiatique, ce que nos meilleurs alliés sont capables de faire pour remporter ces débouchés commerciaux.

- On constate que la guerre en tant que telle est devenue un enjeu très négatif dans l'opinion publique, au moins en Occident. La violence et la mort sur le champ de bataille sont traumatisantes pour des populations qui bénéficient de la paix et de l'abondance depuis près d'un siècle, encore plus lorsque des civils sont touchés (ONG, médias etc.) Comment gérer ce contexte lorsque l'on est justement un acteur qui vend des systèmes et des équipements de défense qui peuvent être utilisés en cas de conflit pour donner la mort, je pense notamment au Yémen où la présence de canons Caesar français a été très critiquée ?

D'abord, l'opinion publique participe aussi au niveau du recrutement des grandes entreprises de la défense. Très clairement, on peut noter aujourd'hui une sensibilité des jeunes ingénieurs à une forme d'éthique. Les jeunes recrues sont très attentives vis-à-vis de leur rôle dans la société. Par exemple, dans le cas du rachat de *Gemalto* par Thales, c'était une entreprise dont les débouchés commerciaux étaient exclusivement axés sur le secteur civil. Lorsqu'elle a rejoint le groupe Thales, entreprise qui vend des systèmes d'arme, mais aussi des technologies civiles, l'absorption a confirmé la nécessaire prise en compte de ces enjeux réputationnels. Il y a une réelle forme d'attention dans les populations sur ces enjeux, au sein même des entreprises qui opèrent dans le secteur de la défense. Je pense que Nexter fait face aux mêmes débats, encore plus même, car ils vendent pour le coup des équipements militaires type chars, blindés, canons, et c'est une réalité.

Les départements éthique, HSE etc de Thales, déclinent des directives jusqu'au plus bas niveau de l'entreprise, et sont portés par le plus haut niveau. Donc l'image de Thales dans l'opinion publique est prise en compte par la direction, avec une conscience de cette sensibilité nouvelle. C'est assez fortement intégré aujourd'hui. On a vu récemment le discours de Patrice Caine (PDG Thales) sur les drones armés par exemple, il s'est montré très clair sur le sujet.

- Effectivement, je n'avais pas envisagé ce risque selon lequel la réputation de l'entreprise influencerait finalement ses recrutements vis-à-vis d'une jeunesse de plus en plus sensible à son impact sur la société

Oui, effectivement, aujourd'hui dans une époque où l'information et les images circulent, on a toute une partie de la population des ingénieurs, mais également des ouvriers et du personnel, qui se pose des questions, de manière légitime d'ailleurs, de type est-ce que je préfère travailler chez Renault, dans une entreprise qui fait de l'automobile ou est-ce que c'est bien d'aller travailler dans une entreprise qui vend des armes ?
L'image que l'entreprise peut donner à l'extérieur est donc importante.

- Sachant que le secteur de l'armement est fortement lié aux couleurs nationales, à quel point la réputation ou la politique internationale de l'État d'appartenance influent-elles sur la capacité à signer des contrats, à séduire les acheteurs internationaux ? Est-ce un avantage ou un fardeau ?

Dans un premier temps c'est très important, car forcément, on ne vend pas des armes n'importe comment et à n'importe qui. Évidemment les déclarations de politique générale et de diplomatie jouent un rôle important dans la structuration des marchés.
Les résultats à l'export d'entreprises nationales sont bien entendu liés à l'effort fourni au niveau politique.
Par ailleurs, les réticences de certains États peuvent impacter le business des autres. Par exemple dans le cas du Yémen, l'Allemagne a émis de grandes réticences sur les exportations vers l'Arabie Saoudite, et lorsque vous avez des composants de systèmes d'arme dans des sociétés comme Thales ou MBDA ou Safran, vous avez eu des blocages à l'export, que ça soit pour le militaire ou le civil. Donc effectivement, ça peut avoir une influence positive ou négative.

- Donc les décisions d'autres États, au regard de l'actualité internationale, vont potentiellement comporter des risques pour la France ?

C'est pareil pour une société comme la mienne, le jour où la France se heurte avec un État, l'industrie d'armement en pâtira. Regardez le marché en Arabie Saoudite par exemple, l'accès à ce marché dépend fortement de la connaissance des règles et des influences locales. Certains pays européens agissent différemment de la France et peuvent parfois avoir des résultats différents.
C'est valable sur d'autres aspects. Le jour où la France se braque ou irait à l'encontre d'une politique d'importance pour les États-Unis, et si le marché américain se ferme et que les américains décident de nous empêcher d'exporter certains composants, c'est une contrainte

qu'il faut toujours envisager. Là-dessus, je vous conseille de prendre contact avec la DGA, Division Internationale, MA (Maîtrise de l'Armement).

- Dans quelle mesure les collaborateurs au sein de l'entreprise constituent-ils une menace pour sa réputation : corruption par exemple ou revente d'informations à un concurrent ? Est-ce un risque important selon-vous ? Comment le réduire ?

Le risque est important en effet. Le réduire passe en premier lieu par la formation et la sensibilisation. Les entreprises sont aussi accompagnées par les services de l'État sur ces questions. La DRSD veille à ce qu'il n'y ait pas de compromission, que les gens soient *clean* et ne fassent pas l'objet de corruption. La DRSD nous accompagne également sur la sensibilisation pour qu'il n'existe pas de fragilité exploitable par d'autres pays (ou des concurrents).
Ensuite, il y a de vraies décisions d'entreprise en matière d'éthique. Et là-dessus, Thales est très clair sur la façon d'entrer sur un marché, sur la transparence à l'export. Il y a des choses à ne pas faire. Ça comprend également le RGPD, la façon d'obtenir et de stocker des bases de listing, la manière d'influencer, d'organiser des évènements. Tout cela est extrêmement règlementé chez nous, et je pense dans le secteur de l'armement en général.

- Cette réglementation ne comporte-t-elle pas des limites parfois, avec des zones grises sur des marchés en Afrique ou au Moyen-Orient où il peut exister des codes claniques ou dynastiques complètement différents de l'approche de transparence juridique occidentale et des normes anticorruption anglo-saxonnes ?

Je ne vais pas faire d'interprétation, mais à mon niveau je n'en ai pas connaissance. Les pratiques culturelles sont bien évidemment prises en compte et analysées. C'est-à-dire que parler à un État A ou un État B en Afrique ne se fera pas de la même manière, et l'identification de qui est le décideur se fait de manière très naturelle. Mais c'est de l'intelligence économique classique, il n'y a pas de compromission. Je pense que la personne qui s'aventurerait dans ce type de manœuvre chez Thales ne resterait pas longtemps à son poste, car c'est très contrôlé.

- Donc il y a vraiment eu une forte prise de conscience sur ces sujets dans l'industrie française ?

Oui très clairement. Et je pense qu'on n'est pas les seuls, c'est très clair et très contrôlé, car on sait très bien qu'il existe un certain nombre d'ONG qui surveillent tout ça, et même au niveau étatique, nous avons des comptes à rendre. Ça va de la justification de toutes les factures à la façon d'inviter et de recevoir le client.
Là-dessus, il faut avoir conscience qu'il y a un processus de contrôle interne qui est vraiment fort, avec des directives à respecter. Et vous êtes obligé de passer par des formations, des modules de sensibilisation, c'est imposé dans le parcours. Je l'ai vécu personnellement en arrivant chez Thales donc je peux vous en parler.

- J'ai entendu parler récemment de l'affaire Bakarat, où Thales est mis en cause par un ancien intermédiaire ? Comment gérer ce genre de situation pour l'image de l'entreprise ?

Non, je n'ai aucun élément là-dessus, je ne sais même pas de quoi vous parlez. Bon après il faut se méfier, car la concurrence ne se gêne pas pour balancer des *fake news*, publier des informations sur des blogs ce genre de choses. Bien sûr, il n'y a jamais de fumée sans feu, mais il faut toujours raison garder, dans le secteur de l'armement, ce type de pratiques n'est pas rare.

- Vous constatez donc que la concurrence peut être amenée à monter des opérations d'influence ?

Oui, bien sûr. Ça fait partie du jeu. En franco-français, il y en a qui ne se gênent pas non plus. Mais même dans le civil c'est pareil. Le travail de fiches blanches etc, c'est un travail d'influence, tout ce qui touche au faire-savoir. Après il faut raconter la vérité, mais ceux qui se mettent à colporter des choses, sont souvent ceux qui sont en position de faiblesse.

- J'ai terminé les questions que j'avais préparées, avez-vous quelque chose à ajouter ? Ou une analyse personnelle, une expérience par rapport à ce sujet ?

Chez nous le marketing fait un gros travail pour que les choses soient bien présentées, avec la com' également. Mais il y a aussi un gros travail de sensibilisation obligatoire. Et ce sont des sujets qui sont très importants. Les notions de compliance et de réglementation sont très contrôlées. Le département éthique de Thales est particulièrement sensible sur ces questions. On a encore eu un séminaire commercial récemment, et nous avons eu un item entièrement dédié à ces thématiques pendant le séminaire.

- Est-ce que vous estimez justement que la communication et l'image comptent beaucoup dans le cycle de vente du produit ?

Ce qui compte le plus c'est la confiance du client. Et cette confiance n'est jamais acquise pour de bon, c'est-à-dire qu'il faut respecter ses engagements auprès du client, sur les performances, sur les coûts, sur les délais.
Mais aujourd'hui, ce qui prime le plus, pour toutes les entreprises de défense, pas seulement pour Thales, après avoir assisté pendant près de 20 ans à la réduction permanente des investissements au travers des précédentes lois de programmation militaire, souvent minimalistes voire de déconstruction : la reprise de commande est un vrai défi pour tous les industriels. Ça passe par la remise en œuvre des compétences, la relance des processus de production, la reprise des contrôles de qualité… Tout cela dans des délais très contraints.
La notion de confiance est structurante. La confiance, ce n'est pas qu'un mot, c'est aujourd'hui, lorsque les armées s'engagent sur des théâtres d'opérations, et qu'on s'engage de notre côté sur la livraison d'une capacité opérationnelle, on n'a pas le droit de se tromper. Donc l'image, elle passe aussi par le respect de ses engagements.

- À ce sujet, j'ai entendu récemment qu'il y avait des débats sur les capacités opérationnelles du F35 ou de l'A400M par exemple ? Qu'en pensez-vous ? Guerre informationnelle autour du programme F35 ?

Pour l'A400M comme le F35, on mesure bien la complexité de ces programmes, l'importance de montages industriels, imposés ou non. Donc lorsqu'un programme est parti un peu de travers dès son départ, c'est dur de le rattraper.

- Est-ce que vous estimez qu'il existe une stratégie d'information ou d'image qui puisse être gagnante dans ce type de situation où justement un programme est mis à mal, la confiance des acheteurs s'étiole ?

Il y a deux cas possibles : soit l'entreprise est unique sur le marché, elle est incontournable, et dans ce cas il faut la soutenir, l'aider pour qu'elle traverse la crise. C'est le cas d'Airbus. Soit il y existe des concurrents capables de fournir des offres plus intéressantes, et dans ce cas on se tourne vers eux, et l'entreprise peut être mise à mal.
Aujourd'hui, de plus en plus, si le produit n'est pas livré dans les temps ou ne donne pas satisfaction, les clients vont aller chercher ailleurs, et même acheter à l'étranger.

B. Annexe 2 : Interview Jean-Paul Cabot – Safran

- Bonjour Monsieur Cabot, pouvez-vous s'il vous plaît vous présenter et nous expliquer votre rôle actuel chez Safran ?

Bonjour, je suis le Directeur des Risques et de la Conformité chez Safran Electronics & Defense (entité du Groupe Safran côté au CAC 40) depuis plus de 10 ans. Je suis en charge, pour la partie risques d'élaborer la cartographie des risques de la société et de nos filiales, de traiter ces risques pour diminuer l'exposition financière et réputationnelle de la société à ces risques identifiés et évalués (probabilité, impact), afin de protéger nos personnels, nos ressources industrielles, nos actionnaires, nos clients et nos fournisseurs.
En ce qui concerne ma fonction de Directeur de la Conformité, ma mission est de protéger la réputation de la société et indirectement celle du Groupe qui pourrait être atteinte de par des allégations de pratiques commerciales non éthiques (corruption, conflit d'intérêts...) conduisant à des lourdes sanctions financières et pénales au travers des lois extraterritoriales (US, UK) et nationale (loi Sapin II).

- Selon vous, existe-t-il des risques réputationnels spécifiques au secteur de la défense ?

Notre implication dans le marché de la Défense, en France et à l'export peut faire l'objet d'attaques infondées et téléguidées d'ONG, de groupes de pression, de concurrents, d'États ... De par nos équipements militaires soi-disant utilisés dans des zones de conflit par des forces étrangères à l'encontre de populations civiles alors qu'ils sont destinés à la défense de pays contre des agressions externes et qu'ils participent grandement à la sécurité des forces françaises engagées en opérations extérieures ou à la défense stratégique de notre pays. Les attaques liées à des accusations infondées de pratiques de corruption peuvent aussi être des armes économiques utilisées par nos concurrents étrangers dont le pays veut favoriser de manière malveillante l'industrie locale.

- Quels sont les enjeux de la Compliance/Conformité commerciale pour Safran ? Selon vous, pourquoi l'éthique des affaires est-elle si importante pour le secteur de la défense ?

Comme expliqué précédemment, les enjeux de la Conformité commerciale sont à la fois réputationnels (pour le Groupe Safran coté au CAC 40) pour éviter les mésaventures de sociétés nationales (Alsthom) dépecées industriellement et impactées financièrement et pénalement (sanctions pénales lourdes) à partir d'une enquête extraterritoriale (USA) liée à des affaires de corruption, mais aussi enjeux financiers par des sanctions exorbitantes et avantages concurrentiels (Airbus vs Boeing) et enjeux de protection de nos savoir-faire industriels et stratégiques et de nos personnels (savoir-faire nucléaire Alsthom dilapidé). Pour Safran nos positions de leader mondial en aéronautique (moteurs, train d'atterrissage), dans la défense (optronique infrarouge, navigation inertielle, drones) sont jalousés par nos concurrents (historiquement US, Israël, mais aussi maintenant Chine, Turquie) qui pourraient utiliser l'arme Compliance pour nous déstabiliser.
L'éthique des affaires (= conformité commerciale) est d'autant plus importante, car très médiatisée (en tout cas en France) par des affaires du passé (Arabie saoudite, Taïwan ; Pakistan, Inde, ...) et étant donné le ressenti défavorable de l'industrie défense par les populations assimilant défense à guerre.

- Quels sont les plans d'action à mettre en place pour avoir une bonne résilience face aux risques réputationnels ?

En particulier pour le risque réputationnel lié à la Conformité, il faut absolument mettre en place une organisation rigoureuse (correspondants risques et conformité dans toutes les Directions, Divisions, filiales), des procédures à appliquer strictement par des personnels formés (Commerciaux, ...), des dispositifs de contrôle permanents (validation des documents échangés, des paiements effectués aux intermédiaires validés par les procédures comme les Consultants, Distributeurs, ... Utilisés à l'export) et de sanctions personnelles (en cas d'écart d'application des procédures (faire travailler un consultant non validé et sans contrat), de conflit d'intérêt (entre un commercial et un client) et de sanctions commerciales (arrêt d'un contrat avec un distributeur, soupçonné de façon documentée, de pratiques de corruption de l'utilisateur final pour qu'il le choisisse de façon préférentielle à un autre intermédiaire).

- Y-a-t-il des zones géographiques ou des pays pour lesquels vous redoublez de prudence avant d'exporter ?

Oui bien évidemment et il suffit de lire/regarder les médias pour savoir que la corruption est un fléau national local dans beaucoup de zones du monde (Asie, Moyen-Orient, Afrique, Amérique du Sud). Nous nous appuyons sur un certain nombre de paramètres pour effectuer une analyse du risque export (indice de corruption du pays, montant du business, rémunération justifiable d'un intermédiaire par rapport à son activité réelle, due diligence/enquête réputationnelle a priori pour tout partenariat commercial à venir), veille et détection permanente de tout soupçon de pratiques non éthiques de nos partenaires export.

- Disposez-vous d'une méthodologie particulière d'analyse pour traiter le risque d'éthique commerciale ?

Voir ci-avant : analyse de risque éthique commerciale formellement documentée, selon un référentiel bien défini (impact, probabilité, niveau de maîtrise du risque), et particulièrement contrôle permanent et veille sur nos partenariats export (consultant, distributeur, prestataires

de service, partenaires industriels). Le directeur de la Conformité a une délégation directe de responsabilité du Président de la société en termes de Conformité, y compris pénale.

- Quels sont les enjeux des audits de conformité ?

Vérifier par un organisme externe et indépendant que tout le dispositif mis en place dans la société auditée (organisation, procédures, outils d'analyse de risque, due diligence, contrôles documentaires et comptables, application des sanctions) est en conformité avec les lois et réglementations extraterritoriales et nationales, afin de protéger la société auditée et le Groupe.
Pour l'AFA, la réalisation extensive et large d'audits de conformité va permettre de démontrer, sur le plan français, qu'un dispositif anti-corruption conforme aux lois est en place dans le panel des sociétés françaises auditées, afin que l'État français puisse discuter/argumenter d'égal à égal (avec des arguments tangibles) avec les administrations étrangères qui étaient plus avancées sur la lutte anti-corruption.

- Pensez-vous que si l'AFA avait existé à l'époque de l'affaire Airbus, ou même de l'affaire Alstom, l'issue et les conséquences auraient été différentes ?

Non par forcément, car sur ces deux affaires, il y avait/a des enjeux industriels nationaux et géopolitiques qui seraient passés/passeront au-dessus auraient été/seront tout de même à charge dans l'instruction des dossiers d'accusation malgré un audit positif/correctif de l'AFA, tant que cette agence (l'AFA) ne commencera pas à auditer des sociétés étrangères pour équilibrer ces pratiques « impérialistes ».

Sources

Livres et revues

Ullrich BECK, ''La société du Risque'', *Alto (Aubier)*, EAN 9782700736793, 25/10/2001

Anne POIRET, ''Mon pays vend des armes'', *les arènes*, ISBN 978-2711201068, 15/05/2019

Fanny COULOMB, ''Industries de la défense dans le monde'', *PUG*, 2017
https://www.cairn.info/industries-de-la-defense-dans-le-monde--9782706126949.htm

Christophe COLLARD, Christophe ROQUILLY, ''Les risques juridiques et leur cartographie : proposition de méthodologie'', *La Revue des Sciences de Gestion*, vol. 263-264, no. 5, pp. 45-55, 2013
https://www.cairn.info/revue-des-sciences-de-gestion-2013-5-page-45.htm

Jean-Pierre SAULNIER, ''L'industrie de défense sous contraintes'', *Stratégique*, vol. 104, no. 3, pp. 69-84, 2013
https://www.cairn.info/revue-strategique-2013-3-page-69.htm

Véronique CHAPUIS-THUAULT, ''L'intelligence juridique ou le droit comme élément stratégique clé'', *Manuel d'Intelligence Économique, 3e édition, Christian Harbulot, puf,* 2019

Philippe TROUCHAUD, ''La Cybersécurité au-delà de la technologie : comment mieux gérer ses risques pour mieux investir'', *Odile Jacoub*, 10/02/2016

Rapports

Rapport 2019 au Parlement sur les exportations d'armement de la France
https://www.defense.gouv.fr/salle-de-presse/communiques/communique_publication-du-rapport-sur-les-exportations-d-armement-de-la-france

Rapport 'La coopération européenne en matière d'armement : un renforcement nécessaire, soumis à des conditions exigeantes'', *Cour des comptes*, 04/18
https://www.ccomptes.fr/sites/default/files/2018-04/20180417-rapport-cooperation-europeenne-armement.pdf

Martial FOUCAULT, Renaud BELLAIS, ''Industrie de défense : un positionnement à trouver'', *CERI*, 2007
https://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_mfrb.pdf

Sitographie

Laurent LAGNEAU, ''L'industrie française de l'armement fait mieux que résister face au rouleau compresseur américain'', *Opex360*, 9/12/2019

http://www.opex360.com/2019/12/09/lindustrie-francaise-de-larmement-fait-mieux-que-resister-face-au-rouleau-compresseur-americain/

''Les dépenses militaires mondiales enregistrent la plus forte augmentation annuelle depuis une décennie atteignant 1 917 milliards de dollars en 2019'', *Observatoire des Armements*, 26/04/2020
http://obsarm.org/spip.php?article336

Michel CARIBOL, ''Dassault Aviation a volé vers un « record absolu » d'activité en 2019'', *La Tribune*, 27/02/2020
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/dassault-aviation-a-vole-vers-un-record-absolu-d-activite-en-2019-840745.html

Ferghane AZIHARI, '' L'industrie de l'armement sclérosée par l'État actionnaire'', *Les Echos*, 14/09/2018
https://www.lesechos.fr/idees-debats/cercle/lindustrie-de-larmement-sclerosee-par-letat-actionnaire-139008

Isabelle CHAPERON, ''La France devient le troisième exportateur mondial d'armement'', *Le Monde*, 09/03/2020
https://www.lemonde.fr/international/article/2020/03/09/la-france-s-affirme-comme-le-troisieme-exportateur-mondial-d-armement_6032277_3210.html

''Défense : envolée des exportations d'armes de la France'', *Capital*, 04/06/2020
https://www.capital.fr/entreprises-marches/defense-envolee-des-exportations-darmes-de-la-france-1340695

''Défense : un « Airbus du naval » indispensable pour résister à la Chine, la Russie et la Corée ?'', *Capital*, 04/02/2020
https://www.capital.fr/entreprises-marches/defense-un-airbus-du-naval-indispensable-pour-resister-a-la-chine-la-russie-et-la-coree-1361356

Guerric PONCET, ''Le Salon du Bourget est-il un nid d'espions ?'', *Le Point*, 18/06/2019
https://www.lepoint.fr/economie/le-salon-du-bourget-est-il-un-nid-d-espions-18-06-2019-2319693_28.php

Antoine IZAMBARD, ''Espionnage : quand la Chine déployait ses grandes oreilles au salon Milipol'', *Challenges*, 22/11/2019
https://www.challenges.fr/entreprise/defense/espionnage-quand-la-chine-deployait-ses-grandes-oreilles-au-salon-milipol_686135

Vincent SATGÉ, ''Note de lecture : L'industrie française de défense'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 01/2016
https://jeunes-ihedn.org/note-de-lecture-lindustrie-francaise-de-defense/

Léna COROT, ''Le drôle de parcours qui a conduit à la fuite de données sur le Scorpène de DCNS'', *L'Usine Nouvelle*, 29/12/2016

https://www.usinenouvelle.com/article/le-drole-de-parcours-qui-a-conduit-a-la-fuite-de-donnees-sur-le-scorpene-de-dcns.N481784

Michel CABIROL, ''Le Qatar près de renoncer au VBCI de Nexter en raison de la mise en examen du patron du PSG'', *La Tribune*, 26/11/2019
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/le-patron-du-psg-mis-en-examen-le-qatar-pres-de-renoncer-au-vbci-de-nexter-833925.html

Nathalie GUIBERT, ''Un contrat de vente de satellites militaires français met au jour les rivalités franco-américaines dans le Golfe'', *Le Monde*, 29/01/2014
https://www.lemonde.fr/international/article/2014/01/29/un-contrat-de-vente-de-satellites-militaires-francais-met-au-jour-les-rivalites-franco-americaines-dans-le-golfe_4356158_3210.html

Enrique MOREIRA, Bruno TRÉVIDIC, ''Airbus chute en Bourse après des informations sur une enquête américaine'', *Les Échos*, 20/12/2018
https://www.lesechos.fr/industrie-services/air-defense/airbus-chute-en-bourse-apres-louverture-dune-enquete-de-la-justice-americaine-240538

Simon CHODORGE ''Un cambriolage près de Dassault Aviation à Saint-Cloud éveille des soupçons d'espionnage, en lien avec les Rafale indiens'', *L'Usine Nouvelle*, 23/05/2019
https://www.usinenouvelle.com/article/un-cambriolage-pres-de-dassault-aviation-a-saint-cloud-eveille-des-soupcons-d-espionnage-en-lien-avec-les-rafale-indiens.N846670

''Airbus : le risque judiciaire diminue, l'action bondit'', *Le Revenu*, 28/01/2020
https://www.lerevenu.com/bourse/valeurs-en-vue/airbus-le-risque-judiciaire-diminue-laction-bondit

Michel CABIROL, ''Réglementation ITAR : la France veut réduire sa dépendance aux États-Unis'', *La Tribune*, 07/09/2018
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/reglementation-itar-la-france-veut-reduire-sa-dependance-aux-composants-americains-789612.html

''Contrôle des exportations de matériels de guerre et assimilés : le dispositif français'', *DGRIS*, 2017
https://www.defense.gouv.fr/dgris/enjeux-transverses/lutte-contre-la-proliferation/controle-des-exportations-de-materiels-de-guerre-et-assimiles-le-dispositif-francais

Claude SERRAFETI, ''L'industrie française de défense'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 2016
https://jeunes-ihedn.org/wp-content/uploads/2016/01/Note-ANAJ-Industrie-De%cc%81fense-2016.pdf

''Thales attaqué par un ex-agent du Golfe**''** *Intelligence Online*, 25/02/2019

https://www.intelligenceonline.fr/renseignement-d-affaires/2020/02/12/apres-l-affaire-barakat-thales-en-difficulte-a-l-export-sans-le-renfort-de-ses-agents,108393448-eve

Michel CABIROL, ''Réglementation ITAR : États-Unis, cet ami qui ne veut pas que du bien à la France'', *La Tribune*, 23/04/2018
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/reglementation-itar-etats-unis-ces-amis-qui-ne-veulent-pas-que-du-bien-a-la-france-776226.html

Raphaël BLERE, ''Guerre économique et justice internationale – l'affaire Airbus'', *Association nationale des Auditeurs jeunes de l'Institut des Hautes Études de Défense nationale*, 05/2018
https://jeunes-ihedn.org/wp-content/uploads/2018/05/DefEco_Guerre-e%CC%81conomique-et-justice-internationale-L%E2%80%99affaire-Airbus.pdf

''Observations du Medef sur la mise en oeuvre de la loi Sapin 2 et la lutte contre la corruption en France'', *Mouvement des Entreprises de France – Direction Internationale*, 10/01/2020
https://www.medef.com/fr/communique-de-presse/article/lutter-contre-la-corruption-guide-de-bonnes-pratiques-destine-aux-entreprises-pour-lapplication-du-volet-anti-corruption-de-la-loi-sapin-ii

Cécile DESJARDINS, 'Fraude et corruption : les multinationales en risque dans leurs acquisitions'', Les Échos, 13/10/2019
https://business.lesechos.fr/directions-financieres/financement-et-operations/fusion-acquisition/030696439222-fraude-et-corruption-les-multinationales-en-risque-dans-leurs-acquisitions-314493.php

Manon LEMERCIER, ''Norme ITAR : l'exposition des technologies françaises aux restrictions américaines'', *Portail de l'IE*, 19/12/2019
https://portail-ie.fr/analysis/2247/jdr-norme-itar-lexposition-des-technologies-francaises-aux-restrictions-americaines

Romain LOUBEYRE, Cédric WELLS, ''ITAR : incidences juridiques et opérationnelles pour les assureurs de risques spatiaux'', *Pratiques juridiques dans l'industrie aéronautique et spatiale*, 2014
http://pedone.info/715-Idest/17.pdf

Emmanuel ROSENFELD, Jean VEIL, ''Le droit, vecteur de la puissance américaine'', *Le Monde*, 01/06/2004
https://www.lemonde.fr/societe/article/2004/06/01/le-droit-vecteur-de-la-puissance-americaine_366971_3224.html

Mathias REIMANN, ''Droit positif et culture juridique : l'américanisation du droit européen par réception'', *Université de Michigan - Archives de Philosophie du Droit*, 2001
http://www.philosophie-droit.asso.fr/APDpourweb/205.pdf

Félix DE BELLO, Ralph MOUGHANIE, ''Une brèche dans l'« impérialisme juridique » américain'', *Le Monde*, 2018

https://www.lemonde.fr/idees/article/2018/10/25/une-breche-dans-l-imperialisme-juridique-americain_5374175_3232.html

''Le Rafale, ce fleuron tricolore au succès commercial tardif '', *Capital*, 08/10/2019
https://www.capital.fr/entreprises-marches/le-rafale-ce-fleuron-tricolore-au-succes-commercial-tardif-1352215

Jérémie SAINT-JALM, ''Les enjeux de la réglementation ITAR dans le blocage de la vente de missiles SCALP à l'Égypte'', *Infoguerre : Centre de Réflexion sur la Guerre Économique*, 01/11/2018
https://infoguerre.fr/2018/11/enjeux-de-reglementation-itar-blocage-de-vente-missiles-scalp-a-legypte/

Hervé GUYADER, ''Vente de Rafale bloquée : la France subit (encore une fois) la loi américaine'', *Les Echos*, 28/02/2018
https://www.lesechos.fr/idees-debats/cercle/vente-de-rafale-bloquee-la-france-subit-encore-une-fois-la-loi-americaine-130796

Bertrand WARUSFEL, ''L'intelligence juridique : une nouvelle approche pour les praticiens du droit'', *Le Monde du Droit,* 2010
http://www2.droit.parisdescartes.fr/warusfel/articles/IntelligenceJuridique_warusfel2010

Bertrand WARUSFEL, ''Intelligence économique et pratiques juridiques'', *Revue de l'Intelligence juridique*, 1999
http://www2.droit.parisdescartes.fr/warusfel/articles/iepratjuridiques_warusfel.pdf

Emma SEURET, ''Une mauvaise communication fait plus de dégâts que l'on ne croit'', *Les Echos*, 20/09/2011
http://archives.lesechos.fr/archives/cercle/2011/09/20/cercle_37828.htm

Valéry MARCHIVE, ''Menace interne : un vrai manque de sensibilisation, mais aussi un réel risque de malveillance'', *LeMag IT*, 03/04/2017
https://www.lemagit.fr/actualites/450416152/Menace-interne-un-vrai-manque-de-sensibilisation-mais-aussi-un-reel-risque-de-malveillance

''Ne laissez pas l'obsolescence altérer dangereusement votre informatique'', *Les Echos*, 12/03/2018
https://solutions.lesechos.fr/tech/c/ne-laissez-lobsolescence-alterer-dangereusement-informatique-9652/

''Lanceur d'alerte : quels risques pour les entreprises après la directive européenne ?'', *Les Echos*, 16/10/2019
https://business.lesechos.fr/directions-juridiques/droit-des-affaires/responsabilite-assurances/0602053845161-lanceur-d-alerte-quels-risques-pour-les-entreprises-apres-la-directive-europeenne-332428.php

Hassan MEDDAH, ‘’Les sous-traitants, le nouveau maillon faible de la chaine de la cybersécurité’’, *L’Usine Nouvelle*, 23/01/2019
https://www.usinenouvelle.com/article/les-sous-traitants-le-nouveau-maillon-faible-de-la-chaine-de-la-cybersecurite.N796835

‘’Airbus ciblé par une série de cyberattaques, la Chine soupçonnée’’, *Les Échos*, 26/09/2019
https://www.lesechos.fr/industrie-services/air-defense/airbus-cible-par-dune-serie-de-cyberattaques-la-chine-soupconnee-1134900

Philippe ALCOY, ‘’Un pare-feu humain, première ligne de défense en matière de cybersécurité’’, *Silicon*, 27/01/2020
https://www.silicon.fr/avis-expert/un-pare-feu-humain-premiere-ligne-de-defense-en-matiere-de-cybersecurite

Marc-Henry BOYDRON, ‘’Cybersécurité : statistiques que toute PME devrait connaître’’, *Cybercover*
https://www.cyber-cover.fr/cyber-documentation/cyber-securite/cybersecurite-statistiques-que-toute-pme-devrait-connaitre

Daniel CODELLA, ‘’Le facteur humain dans la sécurité informatique : quand le manque de réactivité rime avec vulnérabilité’’, *Wrike*, 22/11/2019
https://www.wrike.com/fr/blog/le-facteur-humain-dans-la-securite-informatique-quand-le-manque-de-reactivite-rime-avec-vulnerabilite/

‘’Espionnage : Airbus cible de plusieurs cyberattaques, la Chine soupçonnée’’, *La Dépêche*, 26/09/2019
https://www.ladepeche.fr/2019/09/26/airbus-cible-de-plusieurs-cyberattaques-via-ses-sous-traitants,8439542.php

Jacques CHEMINAT, ‘’Attaques sur Airbus, la sécurité des sous-traitants en question’’, *Le Monde Informatique*, 26/09/2019
https://www.lemondeinformatique.fr/actualites/lire-attaques-sur-airbus-la-securite-des-sous-traitants-en-question-76572.html

‘’Giuseppe Giordo, le supercommercial de la discorde entre Fincantieri et Naval Group’’, *Intelligence Online*, 13/11/2019
https://www.intelligenceonline.fr/grands-contrats/2019/11/13/giuseppe-giordo-le-supercommercial-de-la-discorde-entre-fincantieri-et-naval-group,108381386-gra

Marie-Béatrice BAUDET, Guy DUTHEIL, Chloé AEBERHARDT, ‘’Bataille feutrée entre Airbus et ses intermédiaires’’ *Le Monde*, 18/12/2017
https://www.lemonde.fr/economie/article/2017/12/18/bataille-feutree-entre-airbus-et-ses-intermediaires_5231323_3234.html

Michel CABIROL, ‘’Exportations d'armes : l'Allemagne approuve de nouvelles livraisons au Moyen Orient’’, *La Tribune*, 01/04/2020

https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/exportations-d-armes-l-allemagne-approuve-de-nouvelles-livraisons-au-moyen-orient-844022.html

''Paris suspend ses exportations d'armes vers la Turquie'', *Le Figaro*, 12/10/2019
https://www.lefigaro.fr/flash-actu/paris-suspend-ses-exportations-d-armes-vers-la-turquie-20191012

Pierre-Olivier GOURINCHAS, ''L'hégémonie du dollar risque de durer'', *Le Monde*, 27/09/2019
https://www.lemonde.fr/idees/article/2019/09/27/l-hegemonie-du-dollar-risque-de-durer_6013302_3232.html

Michel CABIROL, ''Sanctions et armement : la realpolitik des États-Unis'', *La Tribune*, 03/10/2018
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/sanctions-et-armement-la-realpolitik-des-etats-unis-792531.html

Michel CABIROL, ''Armement : la France confrontée à un renversement d'alliance en Arabie Saoudite'', *La Tribune*, 02/03/2020
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/armement-l-arabie-saoudite-une-terre-devenue-inamicale-pour-la-france-840917.html

Célia BELIN, Quentin LOPINOT, ''États-Unis - Union européenne : de la compétition à la défiance'', *Vie Publique*, 24/04/2020
https://www.vie-publique.fr/parole-dexpert/273926-etats-unis-union-europeenne-de-la-competition-la-defiance

Aude BOREL, ''Promesse tenue pour le budget de la défense'', *Ministère des Armées*, 30/09/2019
https://www.defense.gouv.fr/actualites/articles/projet-de-loi-de-finances-2020-promesse-tenue-pour-le-budget-de-la-defense

Nicolas VANEL, "Crash du vol MH17 : malgré la crise, les ventes d'armes à la Russie se poursuivent", *LCI*, 23/07/2014
https://www.lci.fr/international/crash-du-vol-mh17-malgre-la-crise-les-ventes-darmes-a-la-russie-se-poursuivent-1554954.html

''Russie : la France "pourra envisager" d'annuler la vente de Mistral, selon Fabius'', *Le Point,* 18/03/2014
https://www.lepoint.fr/monde/russie-la-france-pourra-envisager-d-annuler-la-vente-de-mistral-selon-fabius-17-03-2014-1802405_24.php

Guerric PONCET, "L'indécision sur les Mistral coûte un million d'euros par mois à la France" *Le Point*, 28/07/2015
https://www.lepoint.fr/monde/l-indecision-sur-les-mistral-coute-un-million-d-euros-par-jour-a-la-france-28-07-2015-1953009_24.php

Laszlo PERELSTEIN, “Mistral : Paris a déjà versé les 949,7 millions d'euros à Moscou”, *La Tribune*, 03/09/2015
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/mistral-paris-versera-949-7-millions-d-euros-a-moscou-502227.html

‘’L'annulation de la vente des Mistral à la Russie, deux fois plus coûteuse que prévu ?’’, *FranceTV Info*, 12/08/2015
https://www.francetvinfo.fr/monde/russie/mistral/l-annulation-de-la-vente-des-mistral-a-la-russie-deux-fois-plus-couteuse-que-prevu_1038183.html

‘’Risque de réputation’’, *NovEthic*, 26/02/2020
https://www.novethic.fr/lexique/detail/risque-de-reputation.html

Jean-Baptiste SIPROUDHIS, ‘’La compliance, un instrument éthique de prévention des risques’’, *Atos*, 25/07/2018
https://atos.net/fr/blog/la-compliance-un-instrument-ethique-de-prevention-des-risques-2

Marie VERDIER, ‘’Des blindés français utilisés pour réprimer les opposants en Égypte’’, *La Croix*, 16/10/2018
https://www.la-croix.com/Monde/Afrique/blindes-francais-utilises-reprimer-opposants-Egypte-2018-10-16-1200976325

Sarah UGOLINI, ‘’Français tué à Bogota : la famille pointe la responsabilité de Thales’’, *RTL*, 05/12/2019
https://www.rtl.fr/actu/international/ingenieur-francais-tue-a-bogota-la-famille-pointe-la-responsabilite-de-thales-7799629194

Lilas-Apollonia FOURNIER, ‘’Sous-marins : Naval Group signe le contrat du siècle en Australie’’, *La Croix*, 11/02/2019
https://www.la-croix.com/Economie/Entreprises/Sous-marins-Naval-Group-signe-contrat-siecle-Australie-2019-02-11-1201001783

‘’DCNS victime d'une fuite massive de données sur son sous-marin Scorpène’’, *La Tribune*, 24/08/2016
https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/le-sous-marin-scorpene-dcns-victime-d-une-fuite-massive-de-donnees-593953.html

Dominique GALLOIS, Caroline TAIX, ‘’Enquête française sur une fuite massive de données de la DCNS sur le sous-marin Scorpène’’, *Le Monde*, 24/08/2016
https://www.lemonde.fr/international/article/2016/08/24/enquete-francaise-apres-une-fuite-massive-de-donnees-de-la-dcns-sur-le-sous-marin-scorpene_4987019_3210.html

Cameron STEWART, ‘’Submarine documents leak: $50bn down gurgler if French can’t keep secret’’, *The Australian*, 24/09/2016
https://www.theaustralian.com.au/commentary/opinion/itll-be-50bn-down-the-gurgler-ifthe-french-cant-keep-a-secret/news-story/535be2819009eb7180b468ef5751f7fb

Léna COROT, ‘’Le drôle de parcours qui a conduit à la fuite de données sur le Scorpène de DNCS’’, *L’Usine Nouvelle*, 29/12/2016
https://www.usinenouvelle.com/article/le-drole-de-parcours-qui-a-conduit-a-la-fuite-de-donnees-sur-le-scorpene-de-dcns.N481784

Andrew GREENE, ‘’French submarine program 'dangerously off track' warns report urging Australia to consider nuclear alternative’’, *ABC.net*, 10/03/2020
https://www.abc.net.au/news/2020-03-11/australia-urged-to-embrace-nuclear-submarines/12043444

Mike YEO, ‘’Australia’s Future Submarine, Do we need a plan B ?’’, *Asia-Pacific Defence Reporter*, 10/03/2020
https://asiapacificdefencereporter.com/australias-future-submarines-do-we-need-a-plan-b/

Romain MIELCAREK, ‘’Impuissance ou cynisme face aux ventes d’armes européennes’’, *Le Monde Diplomatique*, septembre 2019
https://www.monde-diplomatique.fr/2019/09/MIELCAREK/60365

Julia GALAN, ‘’Silence, on arme !", #Frencharms: les campagnes contre les ventes d'armes françaises se multiplient’’ BFMTV, 23/09/2019
https://www.bfmtv.com/international/silence-on-arme-frencharms-les-campagnes-contre-les-ventes-d-armes-francaises-se-multiplient-1772977.html