RAPPORT

Analyse de cas

Déstabilisation informationnelle des entreprises

par

Gil ANCELIN
Laurent BARRAT
Christophe CHEKROUN
Jean-Philippe COUMES
Stéphanie DAVIED
Harold HEREDIA
Fahmi MEGDICHE
Rachid RHILAN

MBA Management des Risques, Sureté Internationale et Cybersécurité - MRSIC 1

JUILLET 2018

EGE Ecole de Guerre Economique

EGE Ecole de Guerre Economique

Déstabilisation informationnelle des entreprises

Auteurs
Gil ANCELIN
Laurent BARRAT
Christophe CHEKROUN
Jean-Philippe COUMES
Stéphanie DAVIED
Harold HEREDIA
Fahmi MEGDICHE
Rachid RHILAN

Sous la direction de
Christian HARBULOT

juillet 2018

Sommaire

Liste des Graphiques

1. Rappel du Contexte et des Objectifs

Une étude de Richard Dobbs, Tim Koller et Sree Ramaswamy, présentée dans le numéro hors-série de Harvard Business Review « Les essentiels 2018 », annonce une régression des profits mondiaux des entreprises, qui passeraient d'environ 10% du PIB mondial à 7,9% dans les dix ans à venir. Les principales entreprises touchées seraient nord-américaines et européennes.

Parmi les conseils formulés par les auteurs de l'étude, deux sont particulièrement intéressants et prometteurs de tensions : « s'engager dans la chasse aux talents » côtoie un « être sur leurs gardes » qui sonne comme un avertissement aux entreprises concernées. Cet « appel à la paranoïa », que présentent les auteurs de l'article, rappelle aux chefs d'entreprises qu'il convient d'étendre la surveillance au-delà des limites de l'entreprise.

Au-delà de cette invitation à une exploration moins centrée sur la structure elle-même, les enseignements dispensés à l 'Ecole de Guerre Economique amènent à élargir le spectre des recherches lors de l'examen des secousses dont sont victimes les organisations de façon plus ou moins régulière.

L'Ecole de Guerre Economique analyse depuis vingt ans des attaques perpétrées contre les entreprises, recherchant et analysant les causes, démontant les motivations et les modalités de déstabilisation, identifiant les acteurs derrière les prête-noms et les intermédiaires, dans le but de proposer des stratégies de réponses défensives ou offensives.

Ce « fond documentaire » nous a été confié et nous l'avons complété par l'examen des 43 flashs « Ingérence économique » publiés par la DGSI de juillet 2012 à mai 2018. Lorsque la presse ou l'actualité nous ont fourni des investigations documentées de déstabilisations d'entreprises, nous avons intégré ces données à l'analyse présentée ici.

L'objectif de notre étude est de mettre en exergue les caractéristiques majeures des cas étudiés et d'en présenter une synthèse descriptive. Elle pourrait, dans l'idéal, jouer le

rôle d'un élément de sensibilisation pour tous ceux qui souhaitent rester sur leurs gardes en portant au plus loin la vigilance de leur regard.

2. METHODOLOGIE D'ANALYSE ET PRECISIONS

Nos travaux ont porté sur une centaine d'études de cas, reprenant des cas de déstabilisation d'entreprises dans de nombreux secteurs d'activité et pays. Bien que ces études représentent d'importantes heures de recherche et d'analyse, leur nombre est trop faible pour que nous puissions appliquer une démarche statistique élaborée.

Toutefois, à la lecture de ce fond documentaire, nous avons préparé et alimenté une grille d'analyse destinée à synthétiser les informations présentées dans les études de cas. Nous nous sommes attachés à répertorier les origines géographiques, tant des cibles que des attaquants. Concernant les attaquants, la mise en évidence de leurs rôles, motivations, modes d'action ont complété les questions portant sur l'existence d'une préméditation ou au contraire sur l'exploitation opportuniste d'une faille. Les conséquences sur les cibles ont également constitué un axe d'analyse lors de la réalisation de nos travaux.

Disposant ensuite de ces données structurées de façon plus homogène, nous avons cherché à dégager les tendances reflétées dans ces études et leur éclairage particulier sur les phénomènes de déstabilisation dans le monde des affaires.

Nous tenons à préciser que le fonds documentaire dont nous présentons un éclairage dans cette étude est constitué des publications de deux institutions mobilisées dans la défense des intérêts nationaux, notamment économiques. Cet attachement à la souveraineté nationale se traduit par l'étude et la présentation de cas fréquemment centrés sur la France. Nos travaux mettent cette particularité en évidence, et nous invitons le lecteur à la garder en tête, afin d'éviter un pessimisme excessif.

3. RESTITUTION GENERALE

1. Secteurs d'activité concernés

Nous disposons de deux types de données dans le fonds documentaire objet de cette étude. D'une part, les travaux menés au sein de l'EGE, dont les détails nous ont permis de connaître avec précision l'activité économique exercée par les cibles ; d'autre part, les flashs de la DGSI, rendus volontairement anonymes par souci de confidentialité. Dans ce second cas, les secteurs d'activité ne sont pas systématiquement précisés. Nous avons considéré alors que le secteur d'activité n'était pas déterminant dans le déroulé des faits et que le type d'attaque relaté pouvait concerner tous les secteurs d'activité.

Le graphique ci-dessous présente la répartition des attaques par secteur d'activité, à l'exclusion des 34 cas de portée générale.

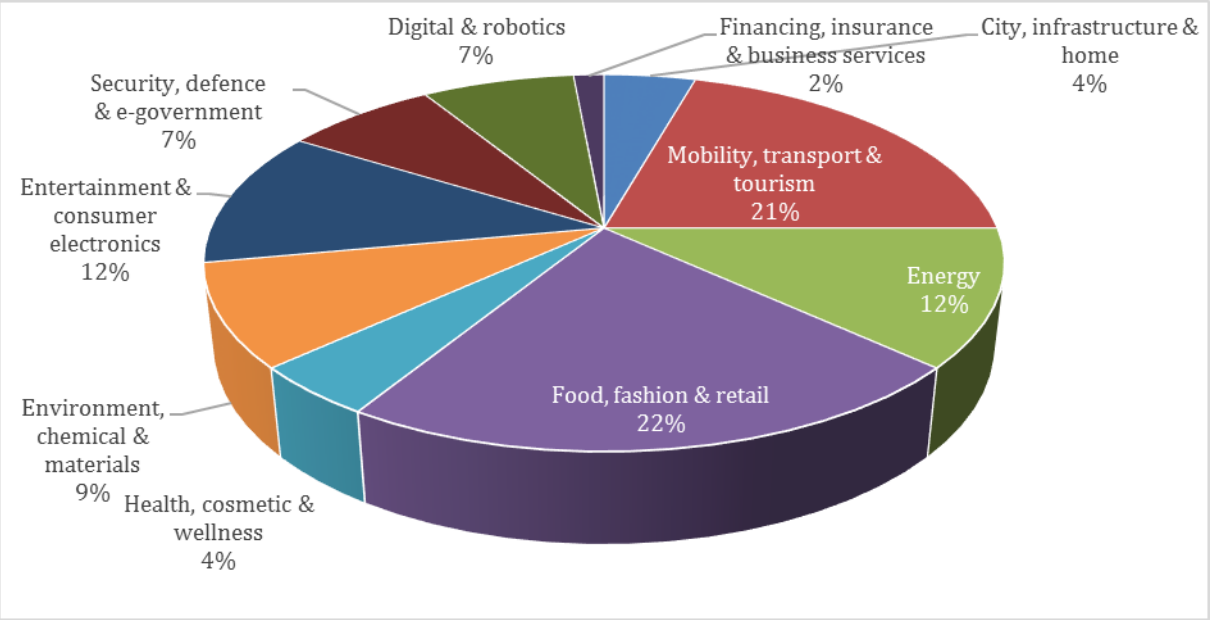


Figure 1 : Secteurs d'activité étudiés

Quatre secteurs se détachent particulièrement, représentant environ 67 % des cas inclus dans cette étude. Il s'agit des activités regroupées autour des thèmes suivants :

- Food, fashion and retail
- Mobility, tranport and tourism,
- Entertainment & consummer lectronics

- Energy

Les informations détaillées sur les trois premiers secteurs d'activité de cette liste sont présentées dans la 6ème partie de cette étude.

2. Approche géographique des protagonistes

Nous abordons ici les origines géographiques des cibles ainsi que celles des attaquants :

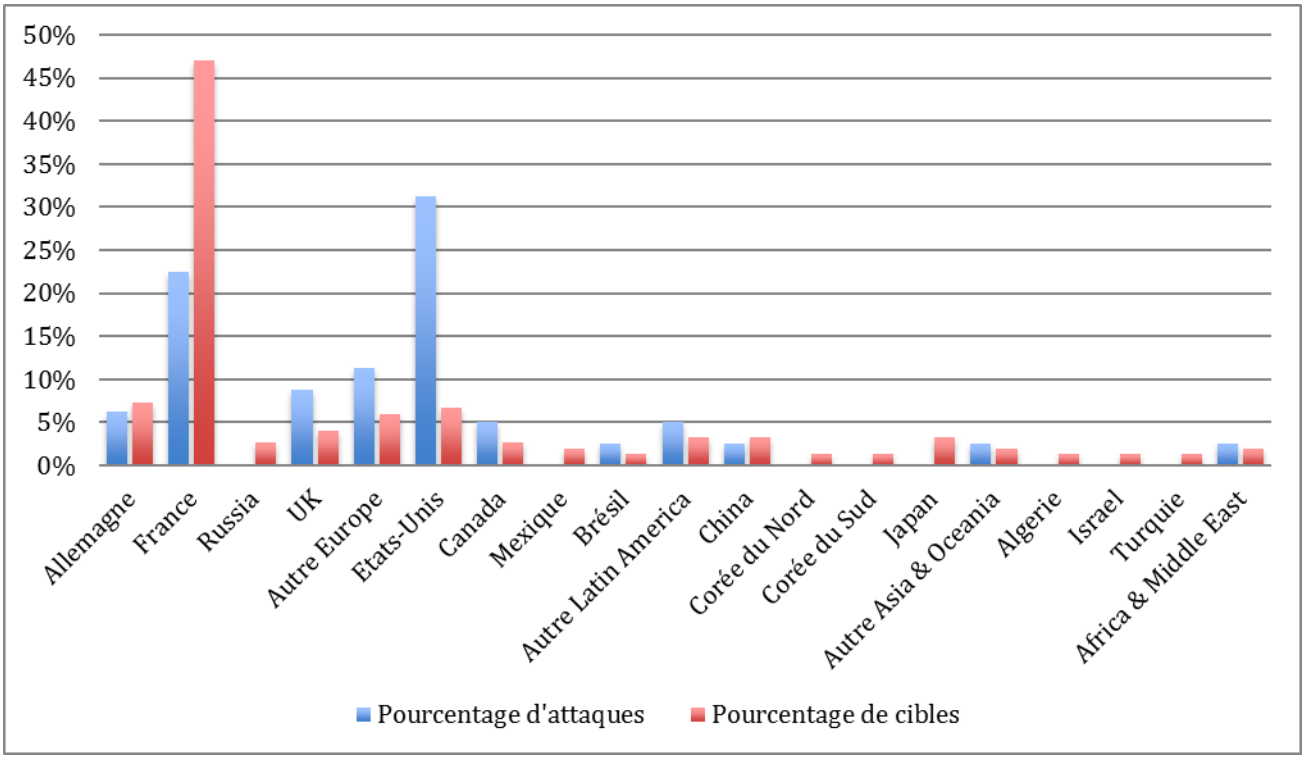


Figure 2 : Répartition géographique des attaquants et des cibles étudiés

Ce graphique met en évidence plusieurs caractéristiques de notre étude. Elle est tout d'abord centrée sur le monde occidental, dans la mesure où la majorité des cas, qu'ils soient abordés sous l'angle de la cible ou de l'attaquant, implique des organisations situées en Europe et en Amérique du Nord.

Par ailleurs, nous constatons l'apparition dominante de deux nations, cible ou attaquante, que sont respectivement la France, visée dans 47% des attaques et les Etats-Unis d'où sont diligentées 31 % des attaques recensées dans le fond documentaire, objet

de cette restitution. Notons également que 22 % des attaques sont menées depuis la France.

Au-delà de la prépondérance de l'Occident parmi les cas étudiés, nous voyons également qu'ils sont essentiellement centrés sur la France. Ceci est lié à aux sources d'informations qui sous-tendent cette étude. Destinées aux entreprises françaises, les flashs d'information de la DGSI ont vocation à développer une culture de la sécurité, en portant à la connaissance des responsables des entreprises, un résumé des affaires constatées en France et de nature à porter atteinte au tissu économique national. Par ailleurs, l'EGE est un établissement de formation français. A ce titre, il pourrait tendre culturellement à travailler de façon préférentielle sur des cas impliquant des entreprises françaises, tant attaquantes que cibles

3. Quelques informations sur les attaquants

Dans l'article de la revue Harvard Business Review que nous citions en préambule de cette restitution, Richard Dobbs, Tim Koller et Sree Ramaswamy invitent les chefs d'entreprise à regarder hors de leurs organisations pour s'adapter aux conditions économiques prévues pour la décennie à venir. Cette position semble se poser comme un écho à la synthèse des cas que nous avons étudiés comme l'illustre ce graphique :

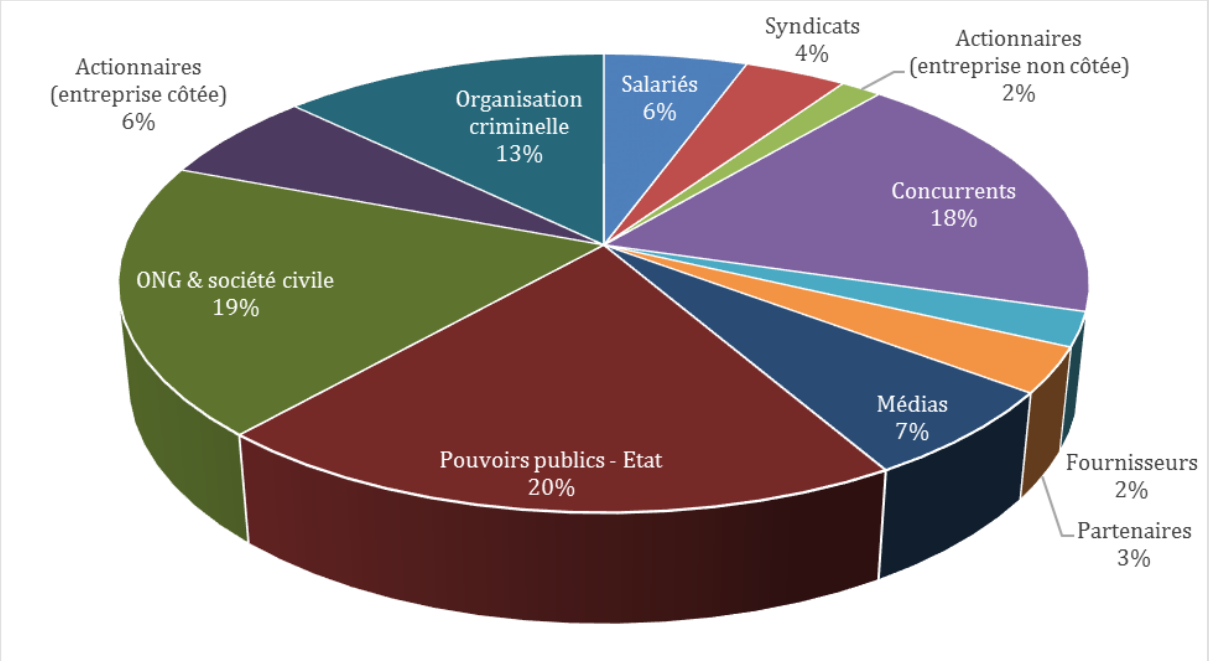


Figure 3 : Rôle de l'Attaquant

En effet, si nous considérons que les salariés, syndicats et actionnaires constituent des protagonistes internes aux organisations, nous constatons que seules 18 attaques sur 100 sont initiées ou menées par ces partenaires internes. Parmi les tiers externes à l'entreprise, nous pourrions trouver trois cercles d'intervenants :

- Ceux que nous pourrions appeler proches, parce qu'ils touchent à l'activité : fournisseurs, concurrents ou partenaires. Ils interviennent pour 23 cas de déstabilisation sur 100,
- Ceux que nous pourrions considérer comme transversaux, parce qu'ils s'intéressent à la population dans son ensemble : pouvoirs publics et Etats, ONG et société civile, ainsi que les médias. Ils sont parties prenantes, initiateurs ou apparaissant comme tels, dans 46 % des attaques que nous avons étudiées,
- Enfin les organisations criminelles, transversales elles aussi, mais que nous isolons de la catégorie précédente en raison de leur côté clandestin, par opposition au statut tout à fait officiel de la catégorie précédente. Les attaques initiées par des organisations criminelles représentent 13 % des dossiers de notre analyse.

L'étude et la compilation des données disponibles dans le fond documentaire étudié nous permet de représenter sous la forme de cet histogramme les motivations des attaquants telles qu'elles ont été identifiées par les auteurs des études.

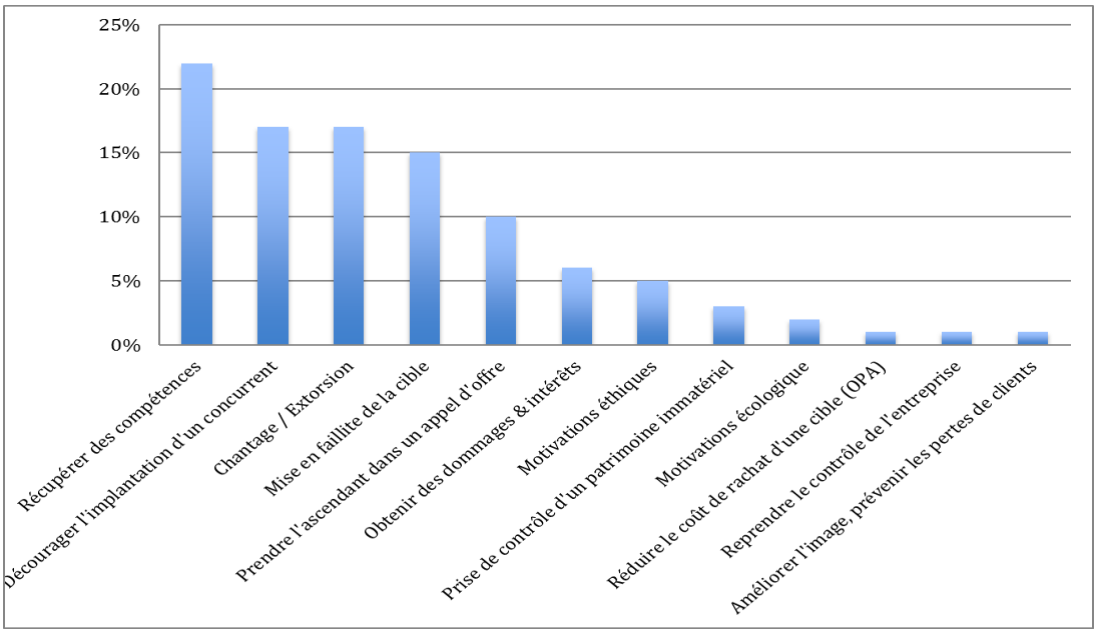


Figure 4 : Motivation des Attaquants

L'observation de ce graphique permet de dégager quelques idées principales.

Parmi les cas étudiés, les motivations liées aux marchés (décourager l'implantation d'un concurrent ou prendre l'ascendant dans un appel d'offres) et à la santé financière (mise en faillite de la cible) restent les principaux moteurs des attaquants, conformément à ce qu'on pourrait attendre d'une étude sur l'insécurité économique. Ces catégories représentent un total de 42 % des cas étudiés.

Le chantage et l'extorsion de fonds restent une motivation fréquente d'attaque, que l'on peut rapprocher de la présence d'organisations criminelles parmi les acteurs significatifs dans les opérations de déstabilisations d'entreprises que nous avons inclus dans cette étude. Les motivations éthiques et écologiques, les demandes de dommages-intérêts pourraient également être mises en perspective avec la forte représentation des ONG parmi les attaquants.

Notons également que le motif le plus fréquent mis en évidence par cet histogramme est le débauchage de compétences clef dans les entreprises visées par des attaques. Cela élargit le sujet de la lutte contre l'insécurité économique au-delà de la seule et directe considération pécuniaire. Les collaborateurs représentent, pour les organisations qu'ils composent, une richesse convoitée et par conséquent à protéger.

L'examen des cas a révélé une multitude de modes d'attaques, qui peuvent toutefois être regroupé dans les sept catégories suivantes :

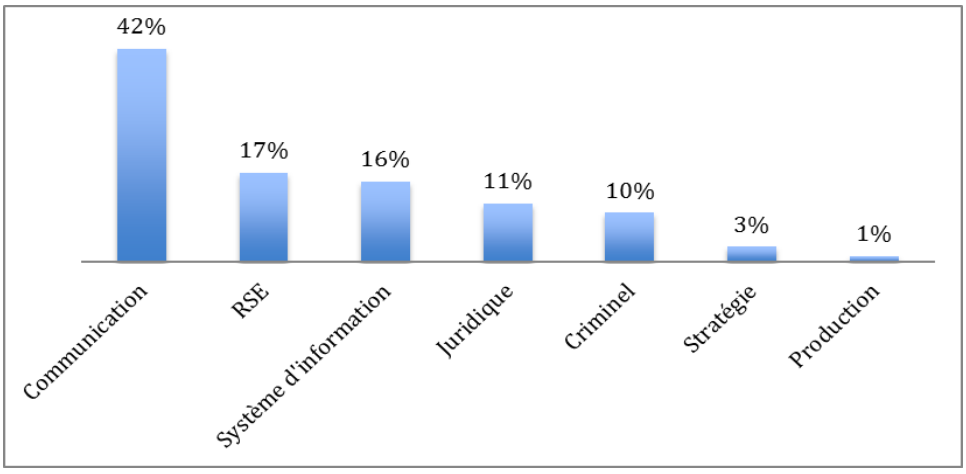


Figure 5 : Répartition des cas par angle d'attaque

Cette classification ne reprend pas de façon exhaustive tous les angles d'attaque qui peuvent exister, mais représente ceux que nous avons rencontrés lors de l'analyse des cas composant le fonds documentaire de cette étude.

Ce graphique présente la communication comme le principal mode de déstabilisation des entreprises en Occident, consacrant la place prépondérante de l'utilisation de l'information dans nos sociétés. S'établissant à 42 % des techniques mises en œuvre, ce que nous avons regroupé sous le chapeau de la communication recouvre de très nombreuses variantes :

- rédaction d'articles négatifs de bloggeurs influents
- campagnes de dénigrement, portant sur les produits, les innovations, la communication, les organes de direction et la stratégie des organisations ciblées,
- soutien des actions d'ONG hostiles aux cibles, qu'il s'agisse d'actions de communication, ou de soutien actif à des mouvements de protestation sociale menées contre les organisations ciblées.

Autre signe des temps, l'évocation de manquements à la Responsabilité Sociale et Environnementale des entreprises est le second vecteur de déstabilisation que nous avons relevé. Il s'agit principalement de dénoncer des négligences dans le respect de la protection de l'environnement, afin de créer une suspicion dans le public.

Déstabiliser une structure par l'attaque de son système d'information représente la troisième modalité d'attaque mise en évidence dans le cadre de cette étude. Ces attaques sont principalement relevées par la DGSI dans les flashs « Ingérence économique ». Citons ici, à titre d'exemple, les rançongiciels qui ont défrayé la chronique au printemps 2017, de façon plus récente les malwares de minage de cryptomonnaies implantés de façon frauduleuse dans les machines des entreprises ou l'utilisation des vulnérabilités des objets connectés pour déjouer la sécurité des systèmes d'information des organisations visées.

L'arme juridique est également utilisée de façon significative parmi les cas de déstabilisation que nous avons étudié. Tous les domaines du droit peuvent être utilisés :

- qu'il s'agisse de droit des sociétés, en organisant la prise de contrôle d'un conseil d'administration en utilisant des moyens légaux,
- qu'il s'agisse de réglementations techniques ou commerciales, en introduisant de nouvelles contraintes réglementaires d'accès à tel ou tel marché,
- qu'il s'agisse d'opérations aboutissant à d'importantes et préjudiciables variations de cours de bourse.

Enfin l'usage de moyens criminels peuvent être mis en œuvre afin de porter des attaques contre les entreprises, ainsi que le met en évidence l'étude à laquelle nous avons procédé. Souvenons-nous que nous avons mentionné les organisations criminelles comme des acteurs significatifs d'attaques. Elles usent d'usurpation d'identité ou de corruption pour créer une faille dans les structures qu'elles visent.

Terminant la revue des modes d'attaques par les actions criminelles, et une idée en appelant une autre, la question de la préméditation des attaques est posée. Dans 84 % des cas que nous avons étudiés, les attaques se sont avérées préméditées. Ceci est probablement lié à la nature de notre fonds documentaire.
En effet, tout au long de cette étude, nous avons relevé une multitude d'intervenants variés, des motivations diverses et des modes d'attaques parfois sophistiqués. Ces actions demandent du temps, des compétences variées et une organisation soignée, autant d'ingrédients constitutifs de la préméditation.

Il n'en demeure pas moins que 16 % des attaques sont opportunistes, c'est à dire qu'elles pourraient être évitées par des mesures préventives, ou par « désamorçage » immédiat dès l'apparition des premiers actes d'attaque.

4. Conséquences pour la cible

Alors que nos travaux ont mis en avant une quarantaine de modes d'attaque parmi les cas étudiés, le nombre de conséquences distinctes ne s'établit qu'à une douzaine.

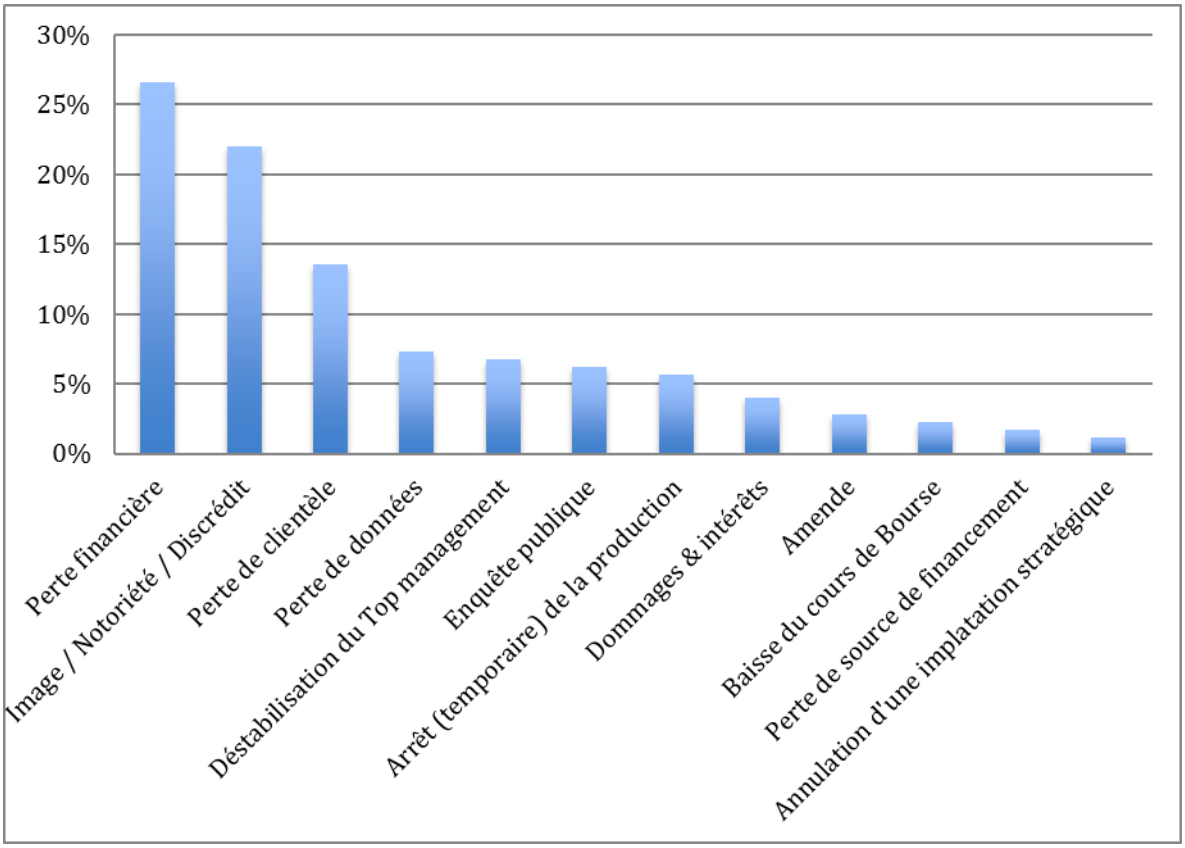


Figure 6 : Conséquences des attaques sur la cible

Des conséquences que nous qualifierions de quantitatives, telle la perte financière, la perte de clientèle, le versement d'amendes ou de dommages-intérêts, la perte de sources de financement côtoient des conséquences plutôt « qualitatives » comme le discrédit, la déstabilisation du top management, le lancement d'enquêtes publiques ou des impacts plus directs sur la stratégie d'entreprise.

Mais il n'en reste pas moins que ces conséquences se nourrissent les unes les autres. En effet, d'importantes pertes financières déstabiliseront nécessairement le management, auront un impact sur l'image et la notoriété de l'entreprise, conduiront à une baisse du cours de bourse, à la perte ou la contraction des sources de financement accessibles, etc.

4. Analyses Sectorielles Detaillees

1. Food, Fashion & Retail

Ce secteur est assez hétérogène, dans la mesure où il intègre des industries agroalimentaires telles que Danone, des industries de la mode et la vente au détail tel que Wal-Mart (nous avons classé ici les cigarettiers). Cependant, la majorité des cas étudiés (86%) provient de l'industrie agroalimentaire.

a. Origine Géographique de la Cible

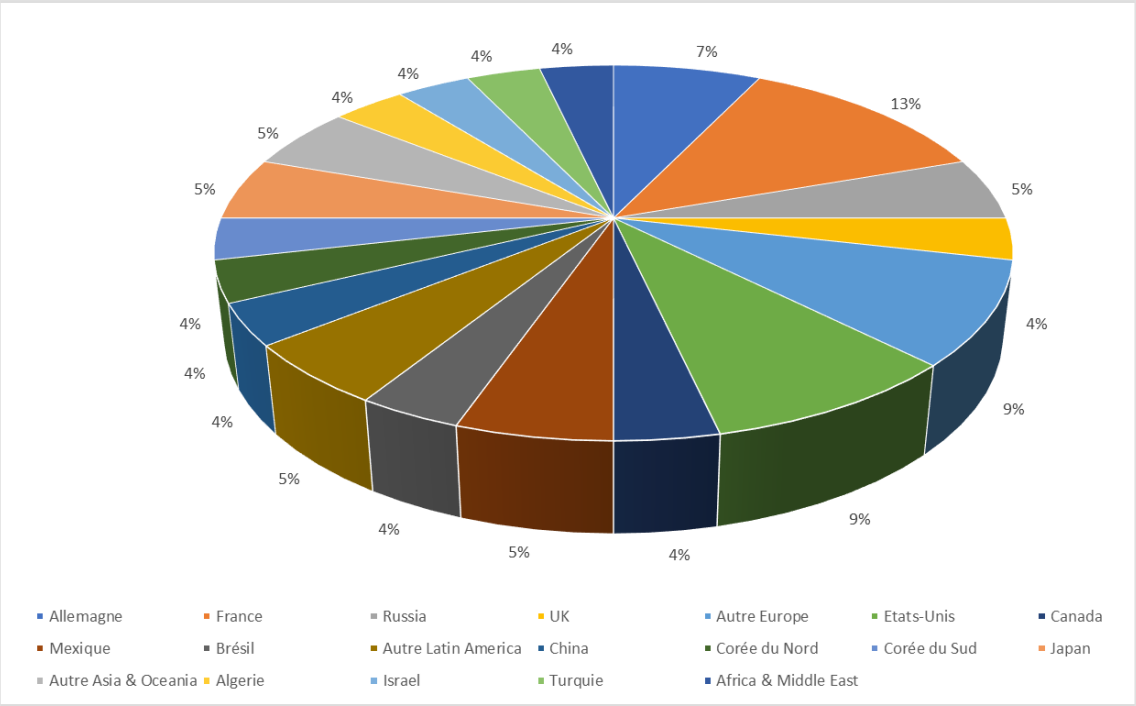


Figure 7 : Origine Géographique de la Cible

A ce stade, il n'est pas possible de tirer une conclusion pour les pays attaqués. Le fait que la France et les Etats-Unis ressortent un peu n'est pas concluant : la majorité des cas étudiés proviennent de cas étudiés en France et les Etats-Unis, pays de la malbouffe, sont plus souvent la cible d'attaque liée à l'industrie agroalimentaire.

b. Origine Géographique de l'Attaquant

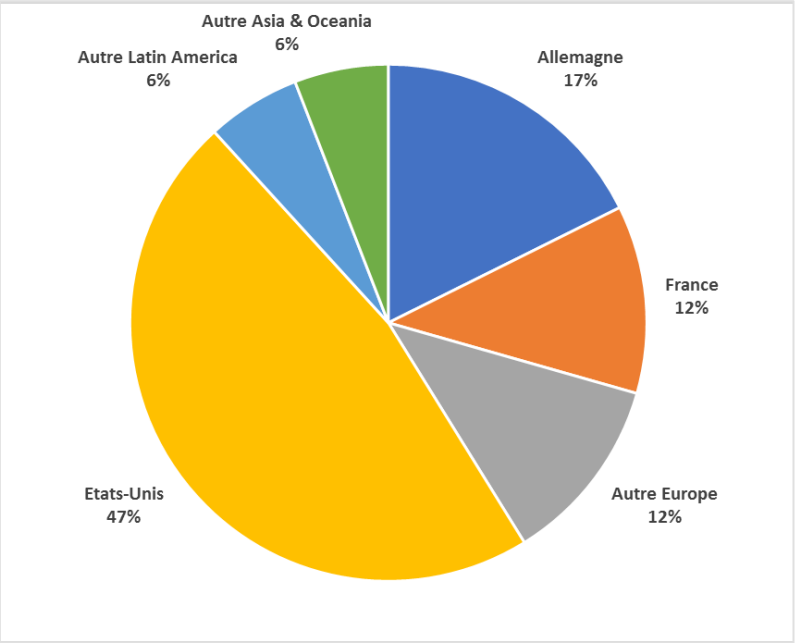


Figure 8 : Origine Géographique de l'Attaquant

Il est intéressant de noter que la moitié des attaques provient des Etats-Unis. Cependant, si l'on regroupe par zone géographique, on constate qu'il y a clairement deux groupes d'attaquants : les Etats-Unis et l'Europe.

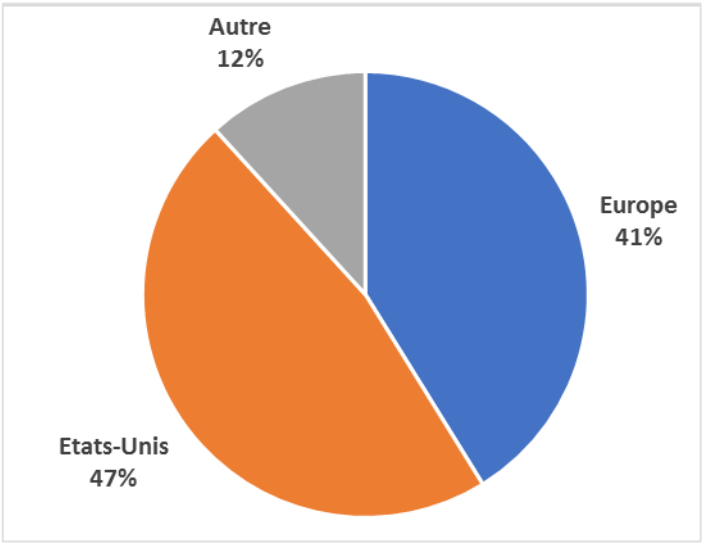


Figure 9 : Zone Géographique de l'Attaquant

Si l'on compare aux origines géographiques des cibles, l'Europe concentre 38 % des attaques, soit presque autant que les attaquants. Cependant, il n'est pas possible de savoir à ce stade s'il y a un lien entre les deux.

c. Rôle de l'Attaquant

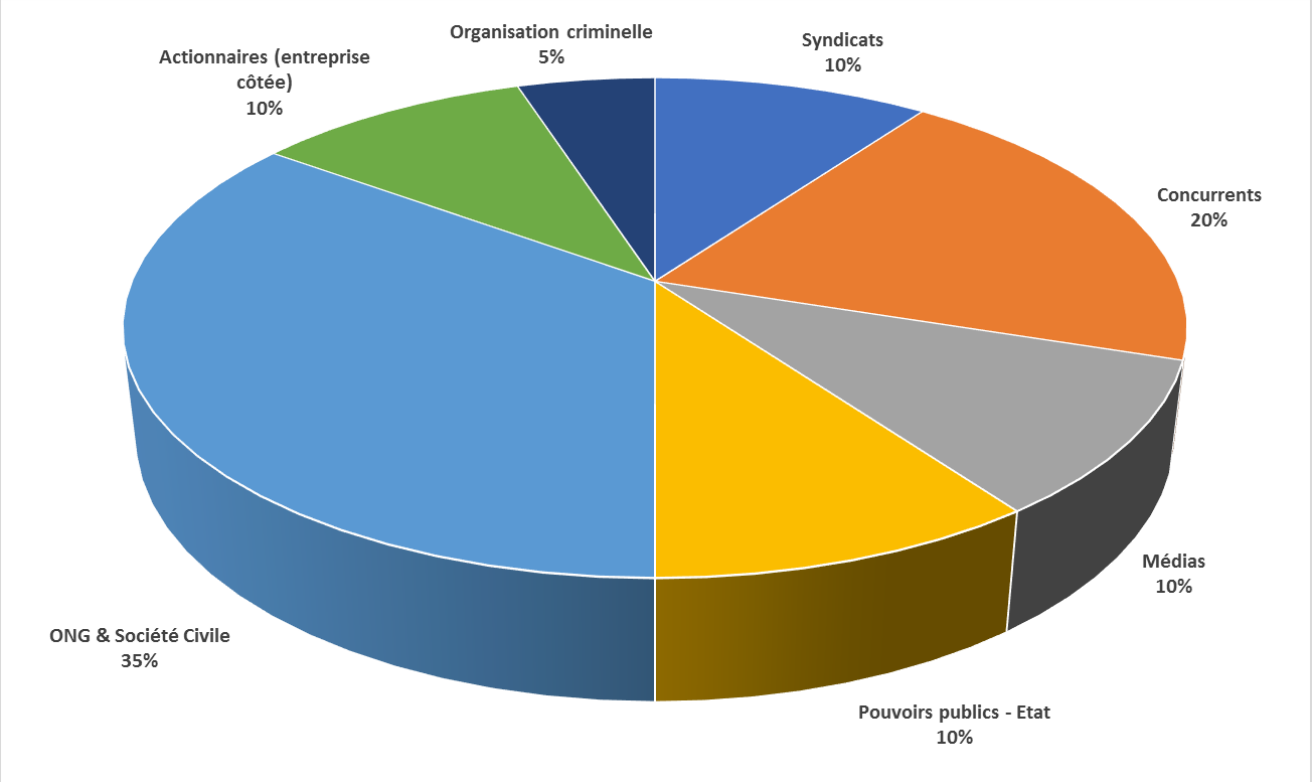


Figure 10 : Rôle de l'Attaquant

On note deux attaquants prépondérants : les ONG & Société Civile ainsi que les concurrents. Cependant, en regroupant les attaquants *financiers* – entreprises – du même secteur d'activité, et en regroupant les acteurs gravitant autour de ces entreprises, ces derniers occupent les deux-tiers du rôle des attaquants. On peut supposer sans trop de difficultés que les concurrents évitent d'agir à visage découvert, et préfèrent utiliser des relais médiatiques, gouvernementaux ou d'ONG par exemple.

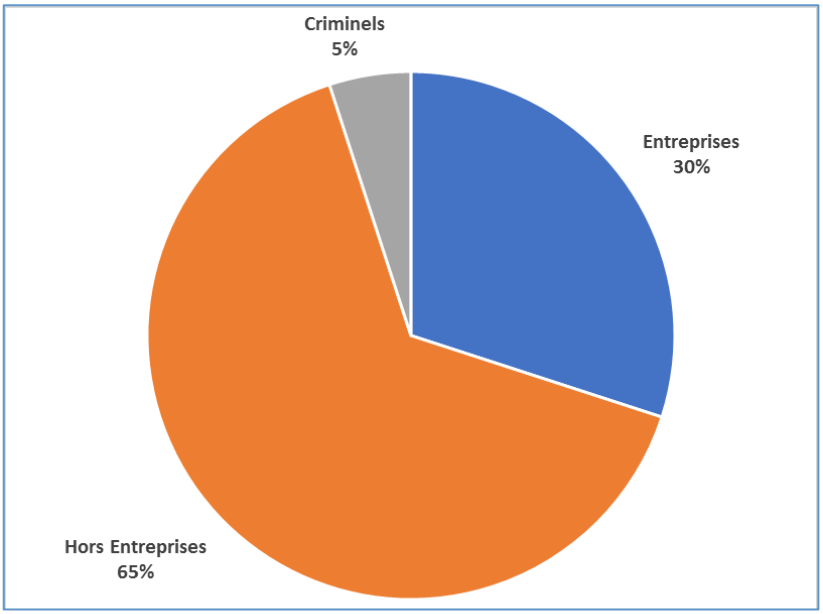


Figure 11 : Grandes familles d'attaquants

d. Motivation de l'Attaquant

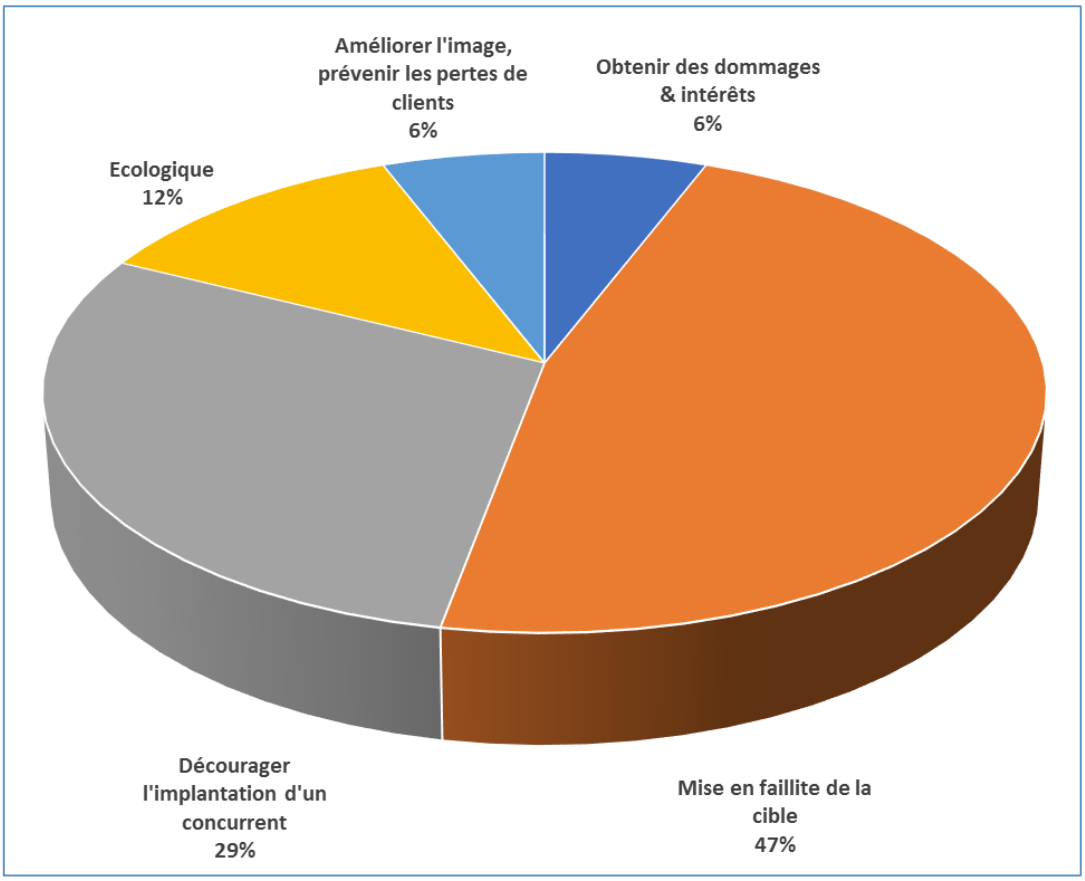


Figure 12 : Motivation de l'Attaquant

Les motivations sont clairement financières, surtout en regroupant toutes les motivations ayant une origine économique. En effet, même dans les cas de mise en faillite ou de découragement du concurrent, ce ne sont pas pour des motifs écologiques ou idéologiques, mais *in fine* pour des motifs financiers.

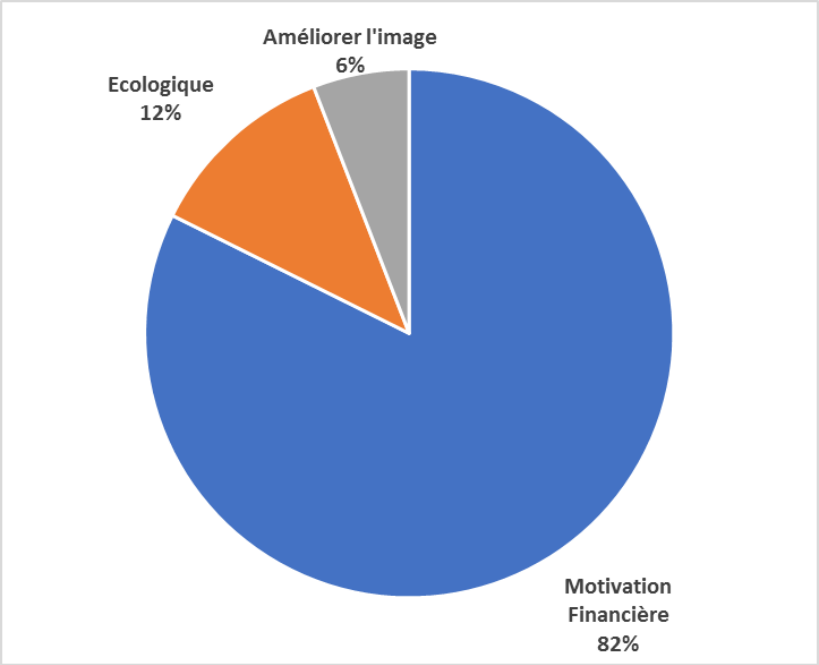


Figure 13 : Motivation d'origine financière

e. Préméditation

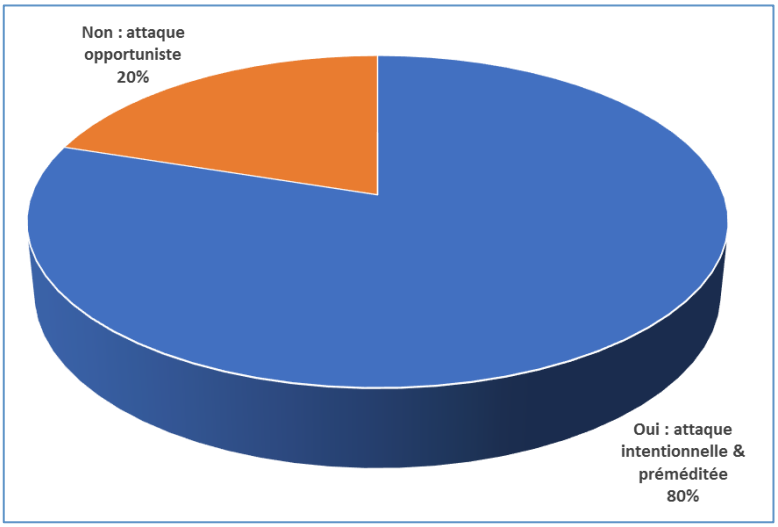


Figure 14 : Préméditation

Bien que les attaques soient variées, 4 sur 5 d'entre elles sont majoritairement préparées et préméditées.

f. Mode d'Attaque

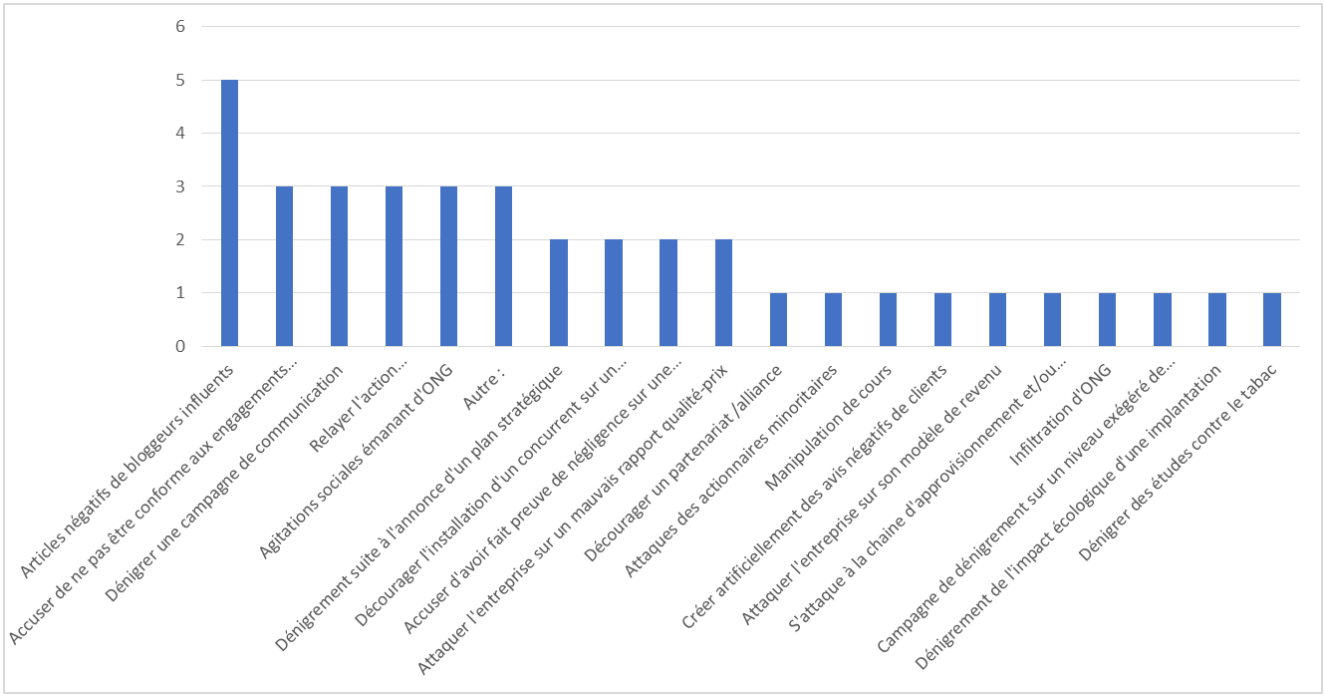


Figure 15 : Le détail des attaques

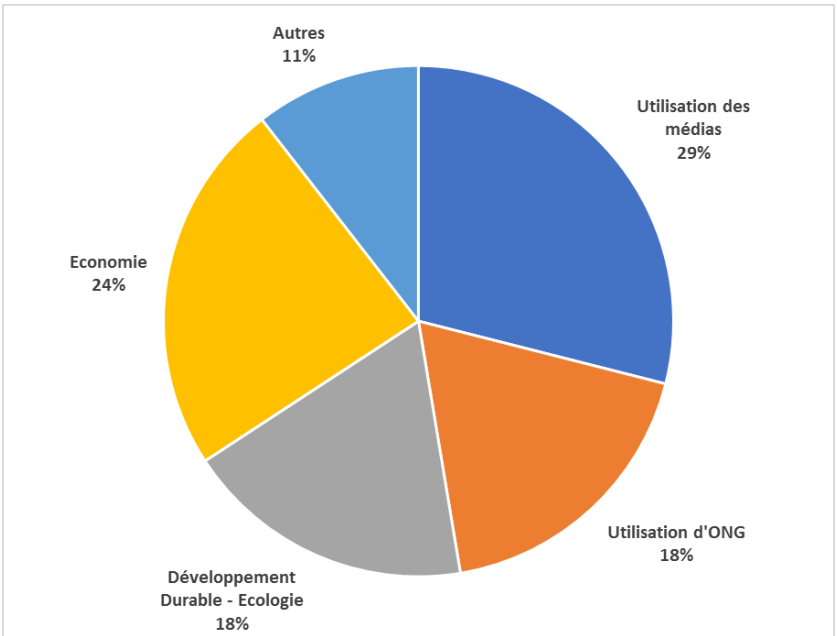


Figure 16 : Synthèse des Modes d'Attaque

On constate que les axes d'attaques sont assez variés. Si les ONG reviennent fréquemment dans les modes d'attaque, elles ne représentent que 18% de ces types d'attaque. Cela n'est pas en corrélation avec le rôle de l'attaquant. Cela signifie qu'une partie des ONG (Attaquant) va utiliser un autre biais que celui de l'ONG pour attaquer. Un axe en plein développement est celui de l'écologie qui recueille un écho favorable auprès des sociétés civiles.

Un des principaux vecteurs d'attaque est par le biais des médias, usant des réseaux sociaux ainsi que les plateformes de blog par exemple. Ces médias-là sont une forte caisse de résonance pour les attaquants. Ensuite il est ensuite possible qu'une ONG ou un concurrent se cache derrière ces attaquants du net. C'est une menace à prendre de plus en plus au sérieux, et la mise en place d'une cellule de veille conséquente et expérimentée, telle que celle qui existe chez Nestlé et surveille 7/24 tous les réseaux sociaux, est fortement recommandée.

Enfin, un autre mode d'attaque utilisé est un affaiblissement financier de la cible, souvent en déjouant l'implantation d'une filiale d'un concurrent ou en la faisant fermer a posteriori lorsque sa propre implantation est en jeu.

g. Conséquences

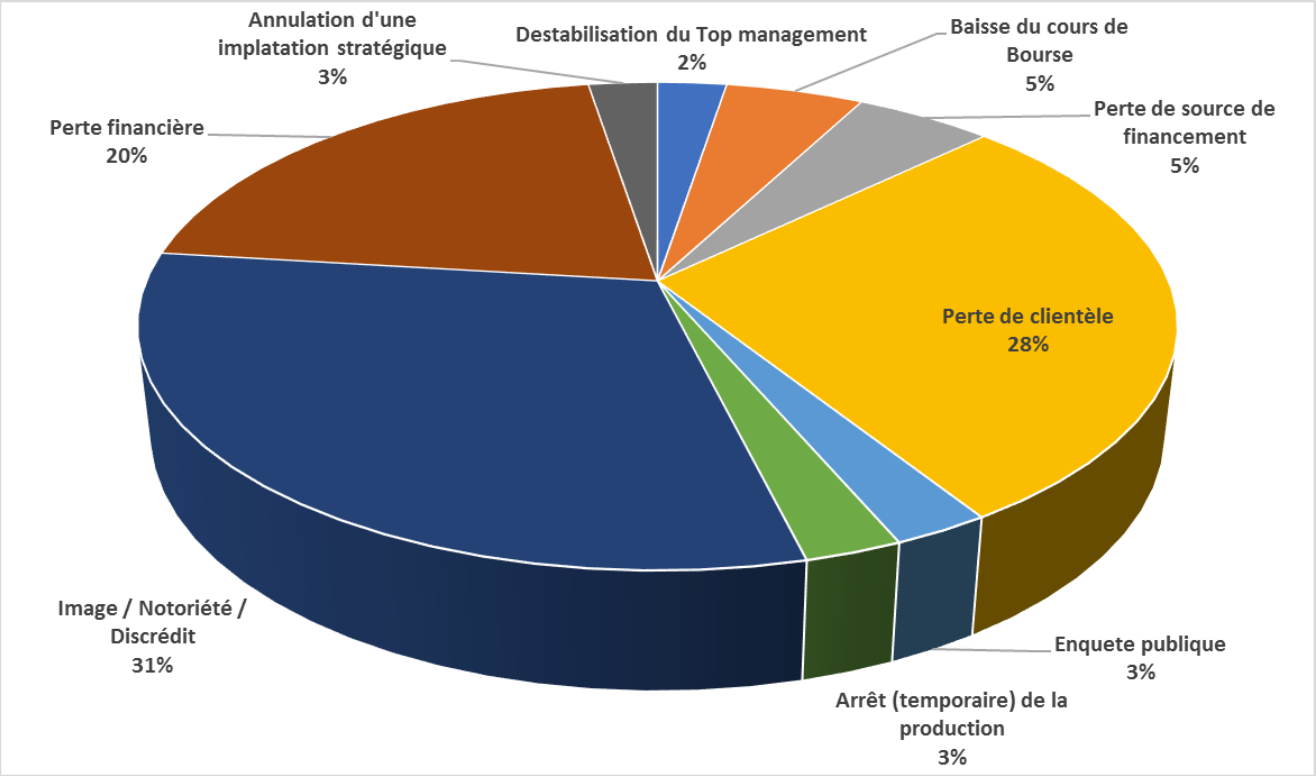


Figure 17 : Conséquences

Les conséquences sont variées, cependant 3 conséquences se détachent immédiatement d'une déstabilisation réussie : un aspect image, un aspect financier et un aspect perte de clientèle, qui peut se conjuguer avec à minima la perte financière. En regroupant les impacts in fine, nous obtenons deux conséquences principales :

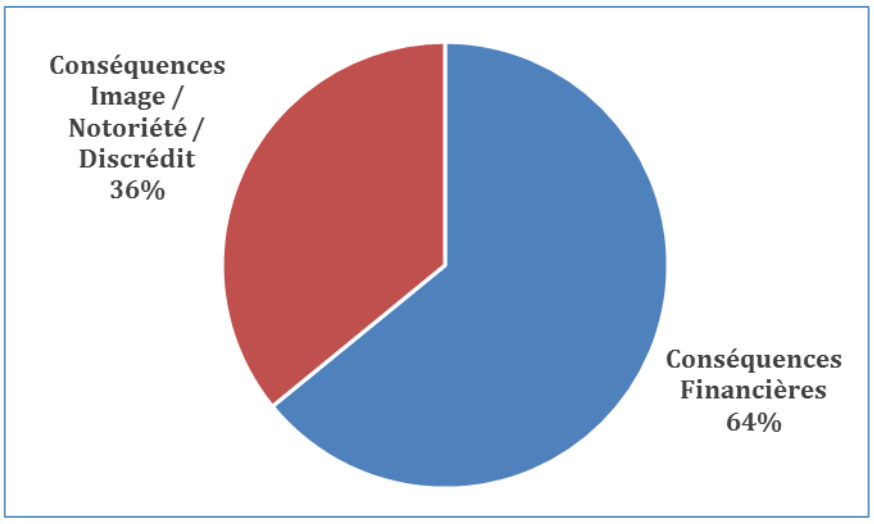


Figure 18 : Conséquences principales

- Des conséquences financières, soit directes, soit comme résultant d'autres conséquences, tels un arrêt de la production ou la baisse du cours de l'action,
- Des conséquences sur l'image ou la notoriété, soit directes, soit découlant d'autres actions, à l'exemple d'une enquête publique.

On note que plusieurs conséquences directes peuvent avoir comme conséquences indirectes une conséquence financière et une conséquence en termes d'image. Nous avons retenu de base les conséquences induites de type finance.

2. Entertainment & Consummer Electronics

Le secteur des télécommunications, que ce soit dans le domaine des infrastructures ou du « device », constitue un enjeu majeur pour les états et fait donc l'objet de manœuvres importantes de déstabilisations.
Deux zones géographiques se distinguent, l'Asie et les Etats-Unis.

- Secteur stratégique, le contrôle des voies de transmission de l'information constitue un enjeu majeur en matière de renseignement et guerre économique
- Le volume de données qui transitent depuis les infrastructures (internet) ou bien depuis les « devices » suscitent la convoitise des états dans un objectif de contrôle de l'information.
- Montée en puissance de nouveaux acteurs chinois qui rivalisent avec les acteurs américains sur leur propre marché avec des velléités de croissance aux Etats-Unis et au-delà mettant en avant des enjeux économiques.

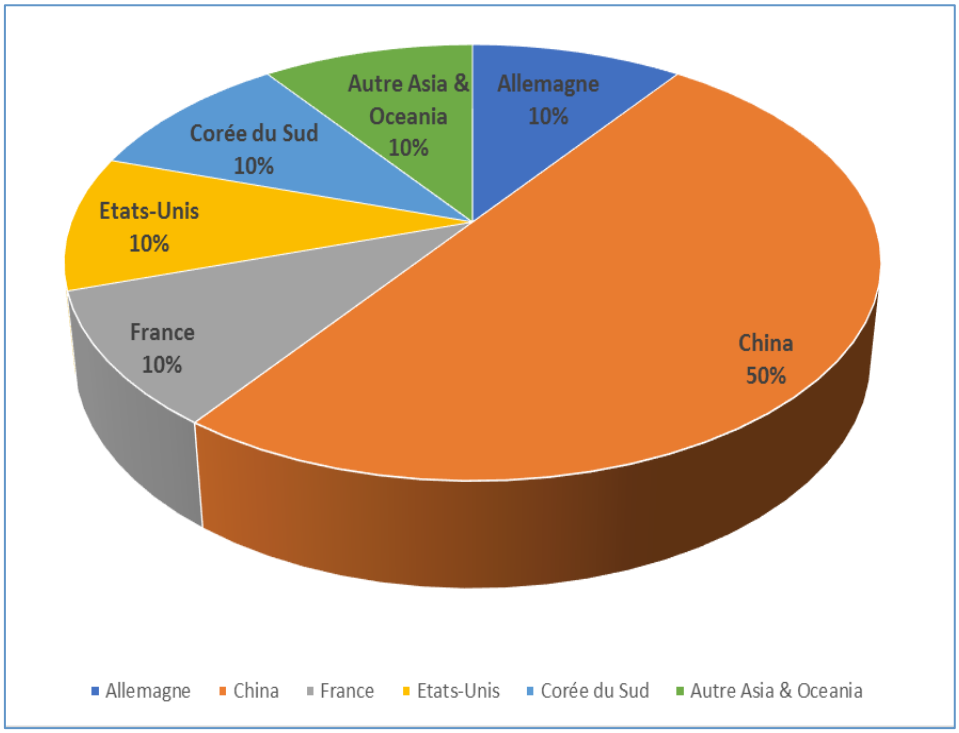


Figure 19 : Origine géographique des cibles

La Chine concentre les principales attaques du fait de sa volonté d'atteindre le « leadership » dans le domaine des télécommunications que ce soit au niveau des appareils ou des infrastructures.

En Europe, hormis Nokia, il n'existe pas d'acteur majeur pouvant constituer une cible prioritaire.

Après avoir conquis son marché local sur les segments du moyen et haut de gamme au détriment d'Apple et de Samsung, la Chine adresse les marchés à l'export.

Elle vient ainsi concurrencer les deux acteurs du marché Apple et Samsung suscitant par-delà des réactions de protectionnisme, des campagnes de dénigrement sur la qualité de ses produits ou leur niveau de sécurité.

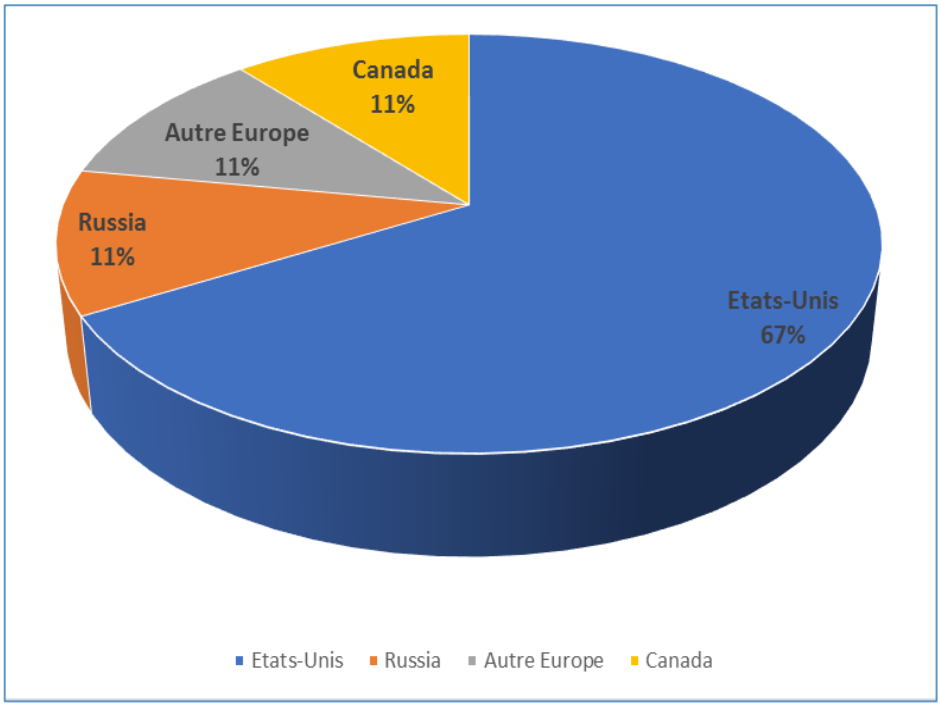


Figure 20 : origine géographique de l'attaque

Les Etats-Unis sont à l'origine de la majorité des attaques orientées vers ses principaux concurrents, qu'ils soient Chinois ou Français, comme cela a pu être le cas d'Alcatel tombé depuis dans son giron, ou les groupes chinois ZTE ou Huawei, souvent attaqués.

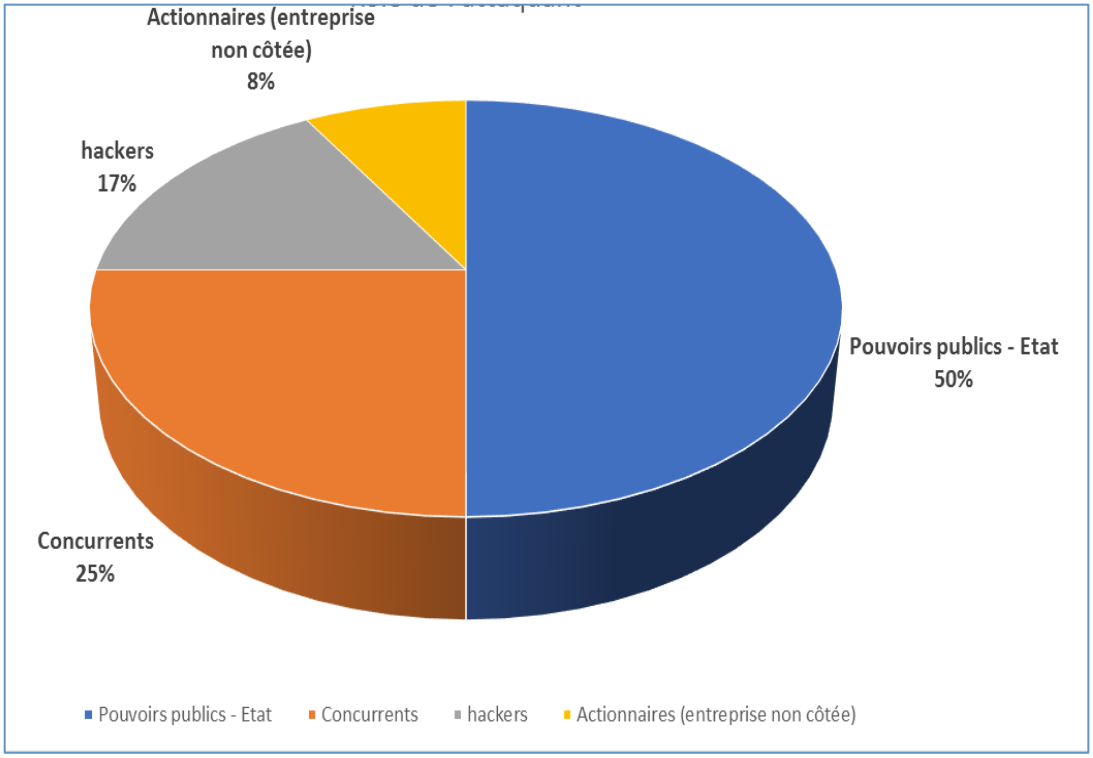


Figure 21 : Rôle de l'attaquant

Les attaques proviennent principalement des pouvoirs publics qui usent de l'arme « respect de la sécurité nationale » pour faire pression sur les opérateurs réseaux télécom américains pour :

- Ne pas acheter des terminaux chinois
- Ne pas fusionner avec des groupes liés aux infrastructures télécoms

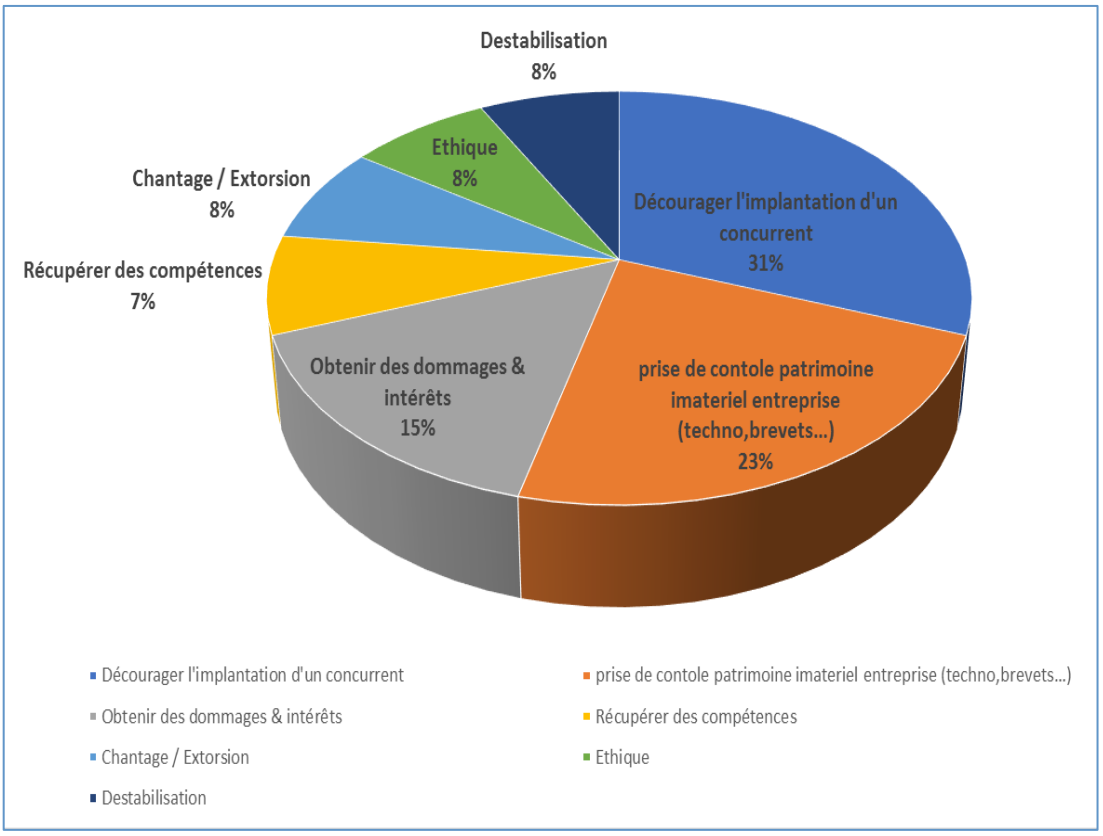


Figure 22 : Motivations de l'attaquant

Sous couvert de politique de sécurité nationale, le principal objectif demeure la protection de son industrie locale et la conservation de la mainmise sur un secteur stratégique : les autoroutes de l'information.

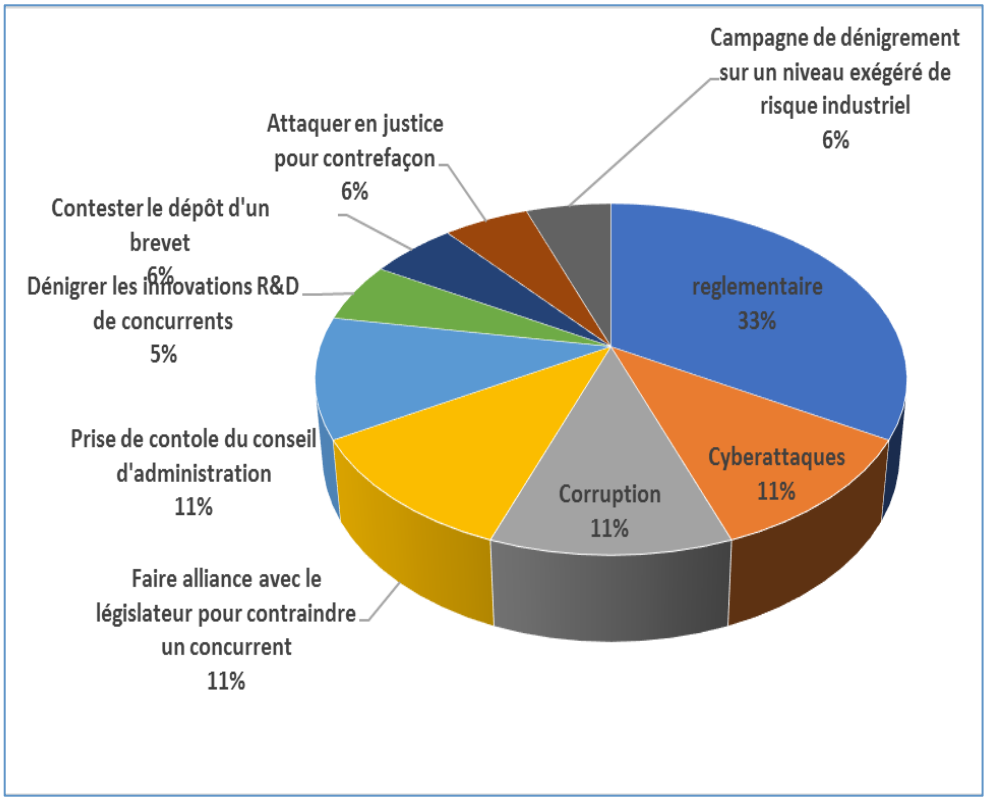


Figure 23 : Mode d'attaque

Les principaux leviers utilisés dans cette guerre économique demeurent le volet règlementaire s'appuyant sur la sécurité nationale, la sécurité et le respect des embargos. Ainsi les Etats-Unis ont utilisé les contraintes juridiques d'accès aux marchés publics pour dissuader certains opérateurs locaux de s'allier ou d'importer des équipements venus de Chine.

Ils utilisent également l'arme de l'extra territorialité de leurs lois pour infliger des amendes aux entreprises étrangères ne respectant pas l'embargo qu'ils ont décrété à l'encontre de l'Iran et de la Corée du Nord.

Ainsi la firme Chinoise ZTE a récemment écopé d'une sévère amende pour avoir vendu des terminaux équipes de processeurs US à l'Iran.

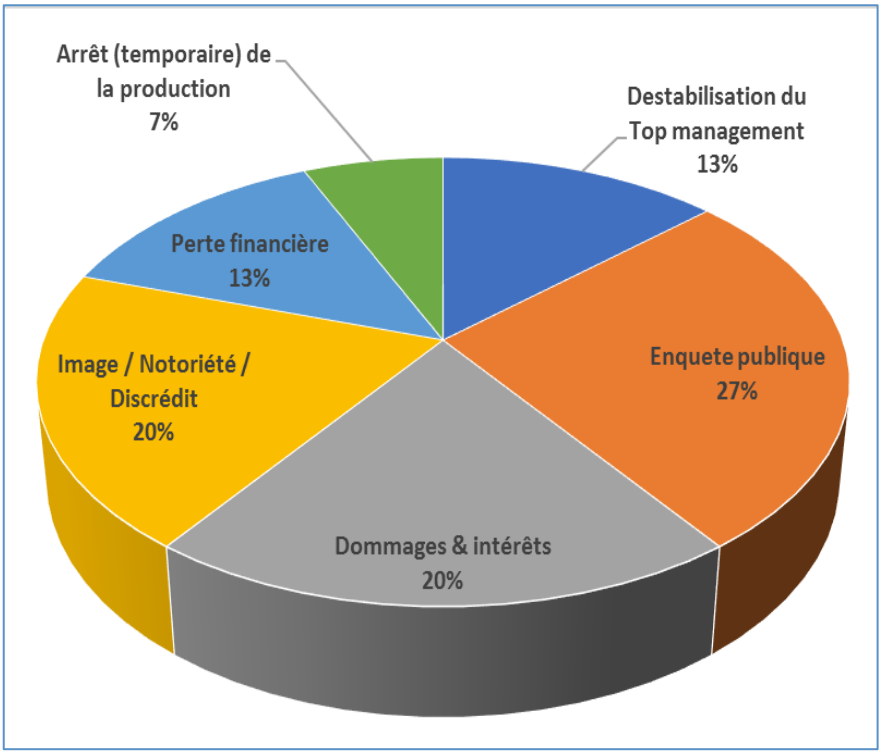


Figure 24 : Impacts sur la cible

Pour les entreprises visées, cela se traduit principalement par des enquêtes publiques destinées à retarder la réalisation des opérations et dissuader les projets de fusion avec un acteur local stratégique, de rachats mais également parfois par la condamnation à de fortes amendes.

3. Mobility, Transport & Tourism

Ce secteur est relativement hétérogène, dans la mesure où il regroupe des industries dont la production est destinée au grand public, tel les constructeurs automobiles, des prestataires de services aux personnes, comme peut l'être la SNCF, mais également des sociétés dont la clientèle est principalement composée de professionnels, à l'exemple d'Airbus EADS, la CMA CGM ou Maersk.

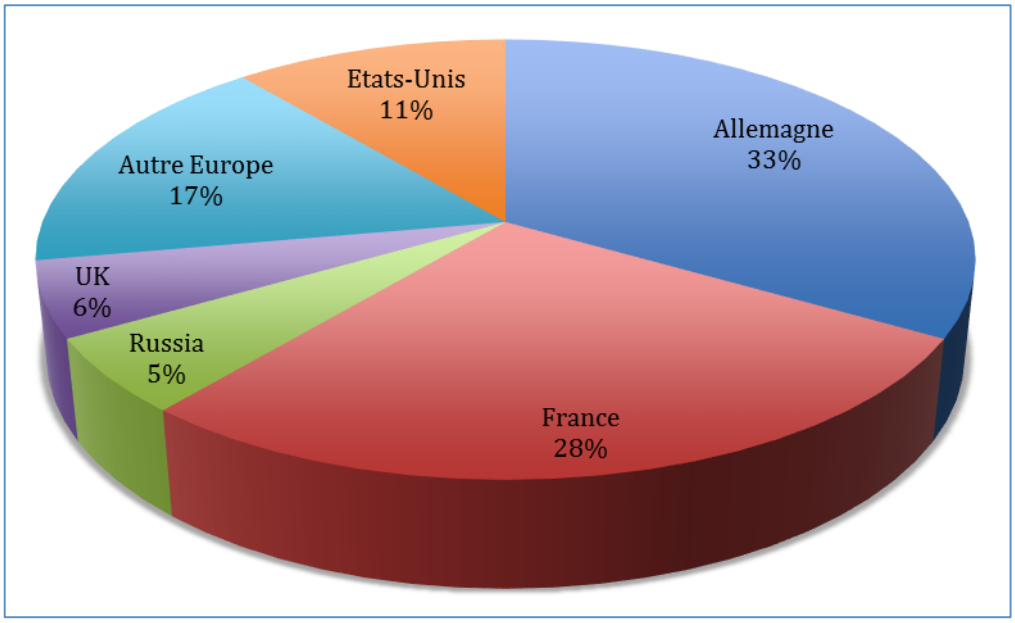


Figure 25 : Origine géographique de la cible

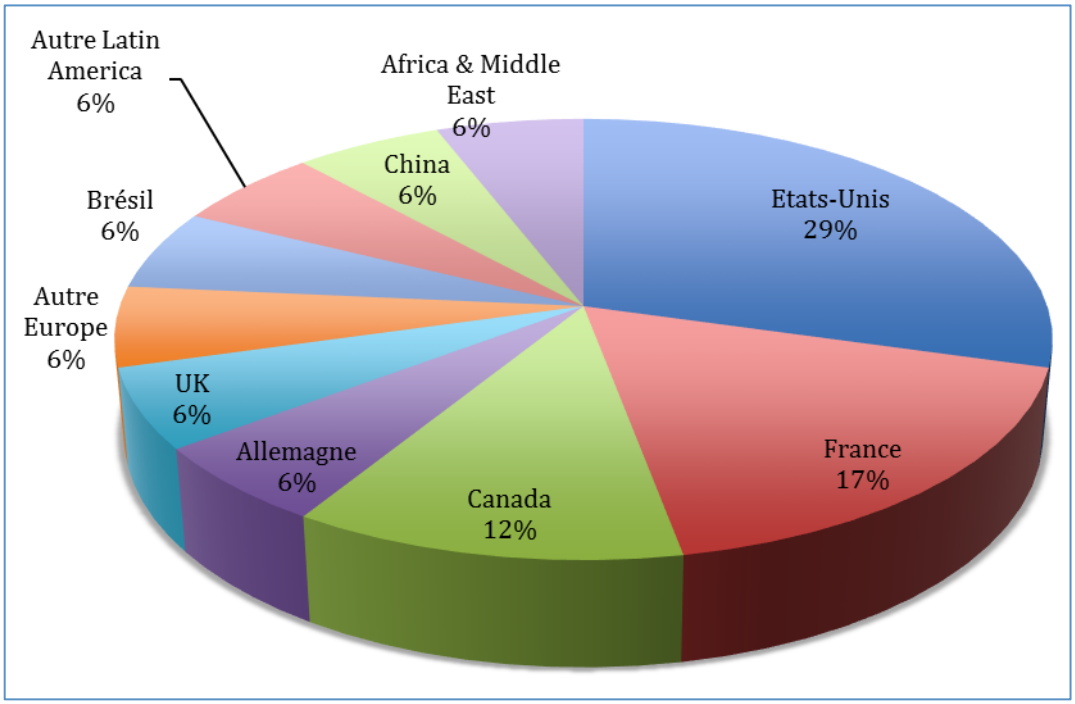


Figure 26 : Origine géographique de l'attaquant

La mise en perspective de ces deux graphiques est plus intéressante que leurs présentations isolées. On constate en effet l'absence de symétrie qu'ils révèlent : alors que les cibles sont essentiellement européennes, représentant 84% des cas étudiés, les attaques sont menées principalement d'Amérique du Nord (41% des attaques lui sont

rattachées), et plus spécifiquement des Etats-Unis. L'Europe est, quant à elle, initiatrice de 18% des cas de déstabilisation étudiés.

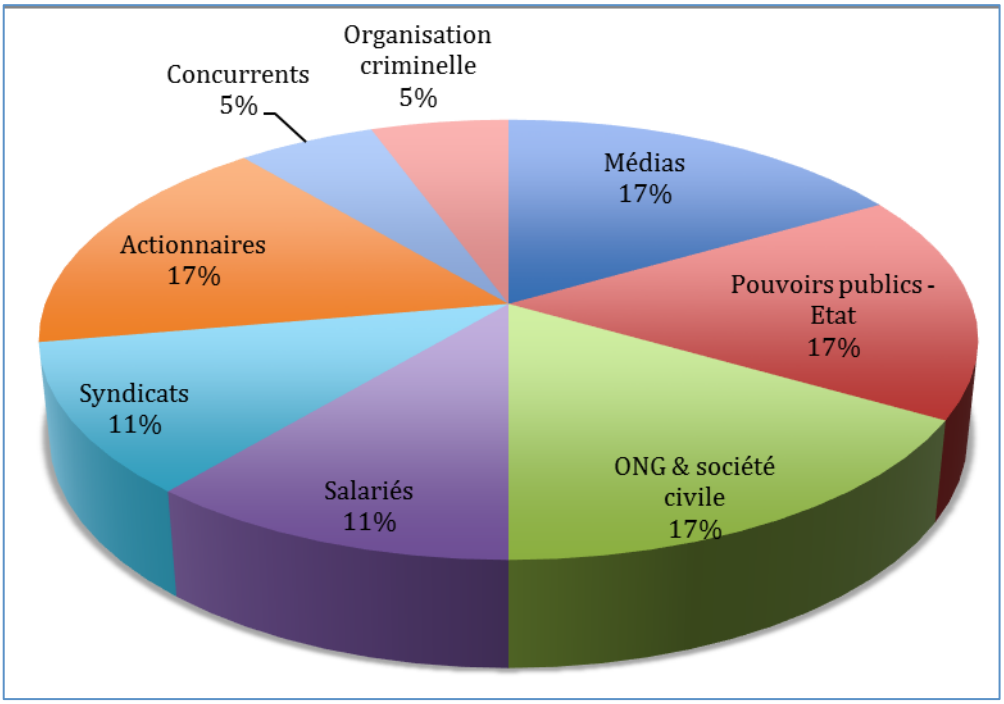


Figure 27 : Rôle de l'attaquant

Les études menées dans le secteur des transports et de la mobilité montrent que les attaquants semblent nourrir un intérêt plutôt indirect. En effet, les parties prenantes en prise directe avec les entreprises, que sont les salariés et leurs représentants syndicaux, les actionnaires ou les concurrents ne représentent que 44% des initiateurs d'attaques. La prépondérance des acteurs externes à l'entreprise pourrait amener à penser que les cibles sont soumises à des attaques ayant trait à des préoccupations relevant de l'intérêt général des populations dont elles assurent la défense ou la représentation. Notons enfin la présence d'organisations criminelles parmi le panel des attaquants.

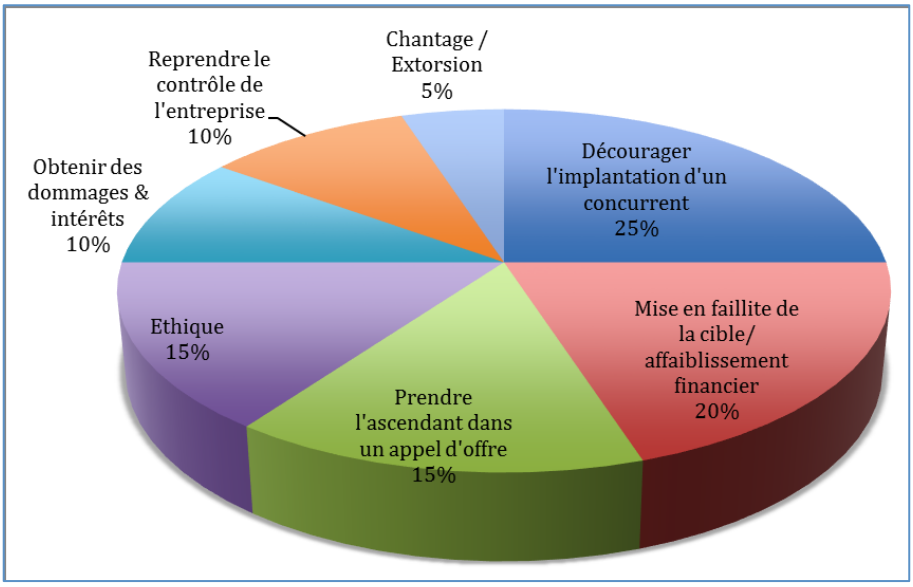


Figure 28 : Motivation de l'attaque

Le graphique relatif au rôle des attaquant ne trouve pas d'écho dans celui qui représente les motivations des attaques. En effet, les motivations « civiles » ne sont représentées qu'à hauteur de 25 % (motivations éthiques et demande de dommages et intérêts), quand le volet commercial représente 80% des motivations.

Ce constat illustre l'intervention importante de la société civile, des médias et des pouvoirs publics dans la sphère économique concernant le secteur des transports et de la mobilité.

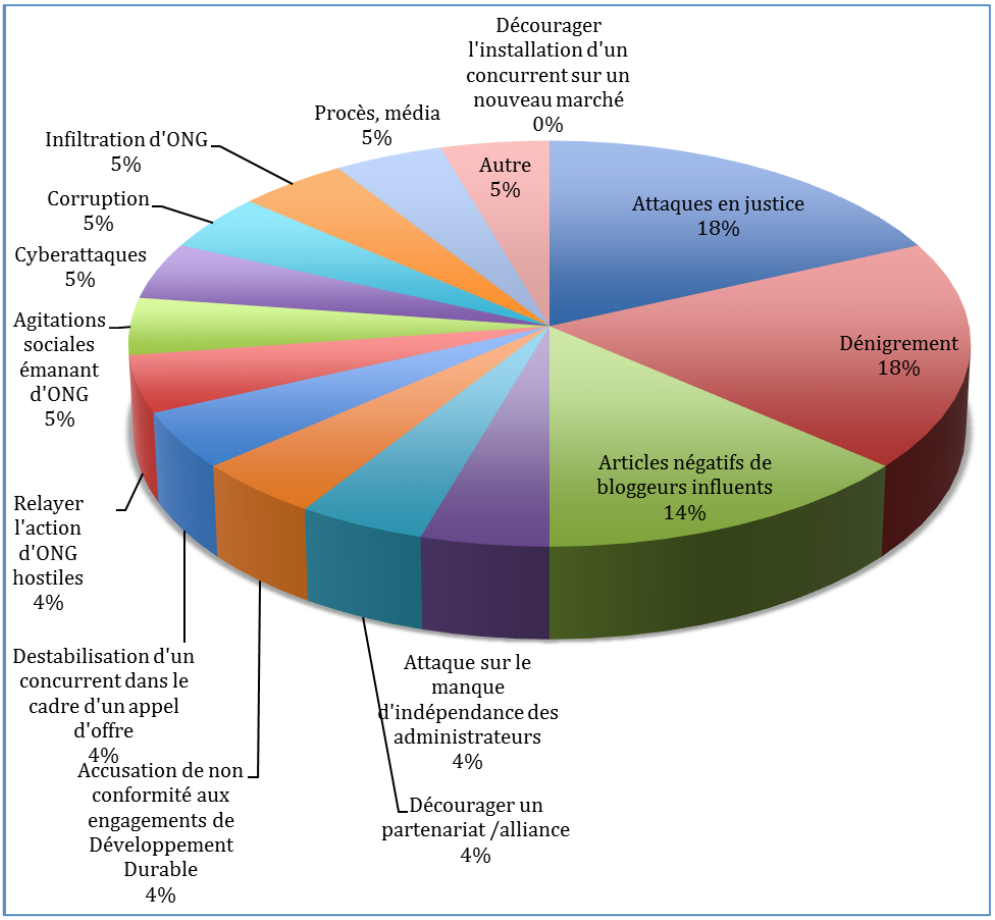


Figure 29 : Modes d'attaque

Alors que les motivations s'articulent autour de deux pôles, économie et préoccupations sociétales, les modes d'attaques se révèlent beaucoup plus nombreux et variés. On peut cependant opposer deux tendances :

- des actions relevant de la guerre de l'information, tels les articles de bloggeurs influents, les campagnes de dénigrement, mais également les accusations de non conformité aux engagements de développement durable, de manques d'indépendance d'administrateurs, ou les actions des ONG qui interviennent sur ces dossiers,
- des opérations plus techniques, telles que des actions en justice, des cyberattaques, ou des interventions destinées à évincer des concurrents lors d'appels d'offres.

Ces dernières actions se révèlent les moins nombreuses dans les cas du secteur des transports étudiés, puisqu'elles ne représentent que 36% des attaques. Cela consacre

donc l'importance des techniques de communication dans l'arsenal de la déstabilisation économique dans ce secteur. Ce point est à mettre en relation avec la typologie des cas qui composent l'étude. En effet, environ le tiers des affaires relatées dans ces études de cas concernent des sociétés dont la clientèle est majoritairement composée de particuliers. Groupe par essence hétérogène, le moyen le plus efficace de le toucher est de passer par la diffusion d'information via internet, la presse ou les caisses de résonnance que constituent certaines ONG.

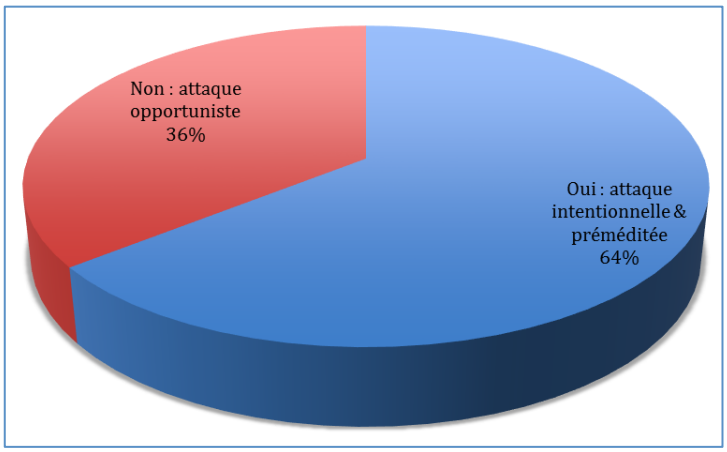


Figure 30 : Types d'attaque

Bien que tous les modes d'attaque ne soient pas nécessairement très techniques comme peuvent l'être des actions en justice ou des attaques informatiques, les actions de déstabilisation que nous avons intégrées à cette étude sont majoritairement préméditées. Près du tiers restent cependant des attaques opportunistes.

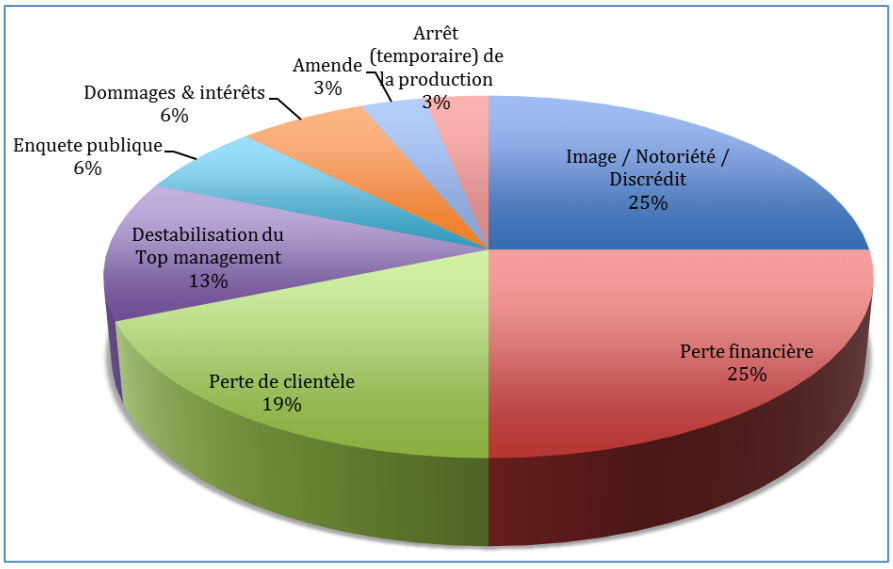


Figure 31 : Conséquences de l'attaque

Les conséquences principales constatées dans le secteur de la mobilité et des transports s'articulent autour de deux axes :

- l'axe économique qui se traduit à court ou moyen terme en perte financières, qu'il s'agisse de perte de clientèle, d'arrêt de production, d'amendes ou de versement de dommages et intérêts,
- un axe plus immatériel qui comprend la perte de notoriété et toutes les atteintes à l'image des sociétés concernées, dont font partie les enquêtes publiques, mais également les actions de déstabilisation du top management.

Les conséquences économiques directes sont les plus représentées dans le panel de cas que nous avons inclus dans cette étude, puisqu'ils concernent 56 % des cas relevés. Cependant, de nombreux cas combinent des conséquences économiques directes et à court terme avec des impacts dont la portée peut être plus longue dans le temps, telles que le discrédit ou la déstabilisation du top management.

5. SYNTHESE DES FLASHS « INGERENCE ECONOMIQUE » DE LA DGSI

Chaque mois, la DGSI prépare et diffuse un flash Ingérence Économique basé sur l'analyse des rapports d'étonnement remontés du terrain par les entreprises françaises. Ces flashs sont rendus anonymes afin de protéger l'identité des entreprises qui transmettent les informations.

1. Origine Géographique de la Cible & Secteur d'activité de la Cible

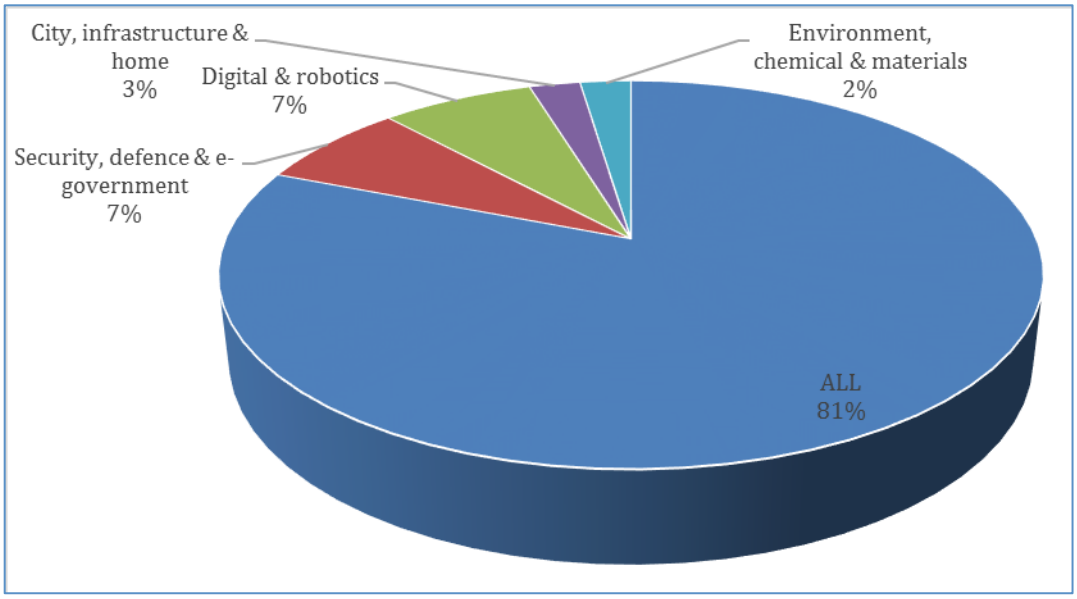


Figure 32 : Secteur d'activité de la cible

Etant donné que les flashs Ingérence Economique sont anonymes, nous ne pouvons établir très clairement une typologie de cible par secteur d'activité. Ceci étant dit les cas traités sont assez génériques pour considérer que toute entreprise française peut être la cible des attaques décrites.

2. Origine Géographique de l'Attaquant

Le fait que ces flashs Ingérence Economique soient produit par un organisme gouvernemental empêche de désigner l'origine de l'attaque dans un tel document, il n'y a donc que très peu d'information à ce sujet.

3. Rôle de l'Attaquant

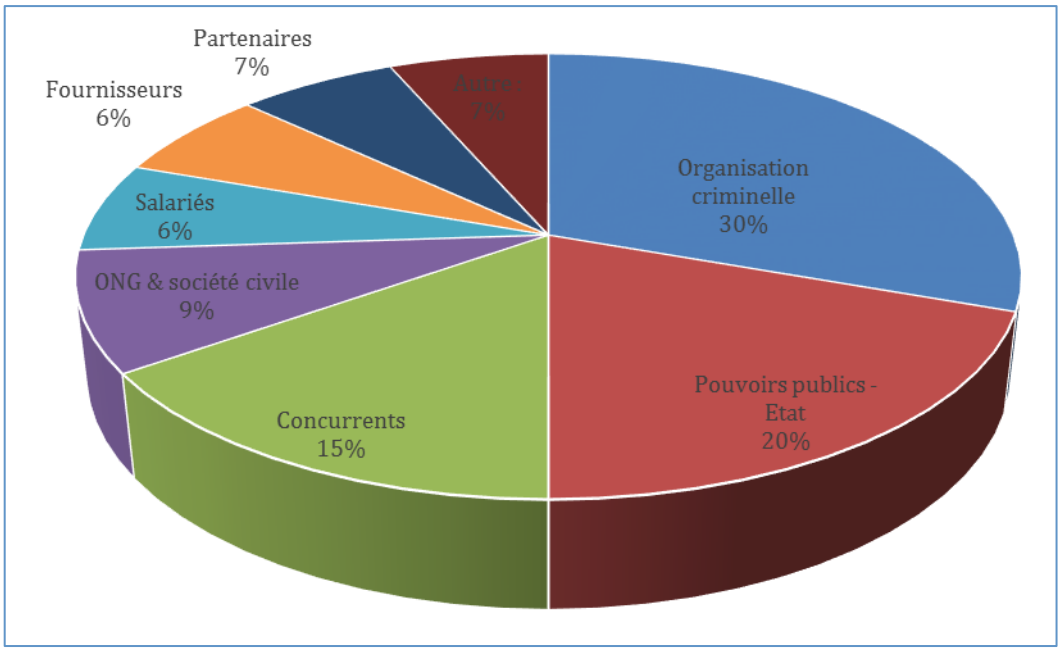
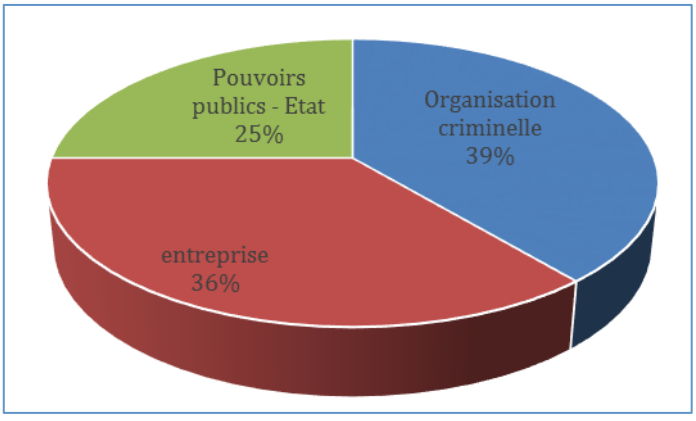


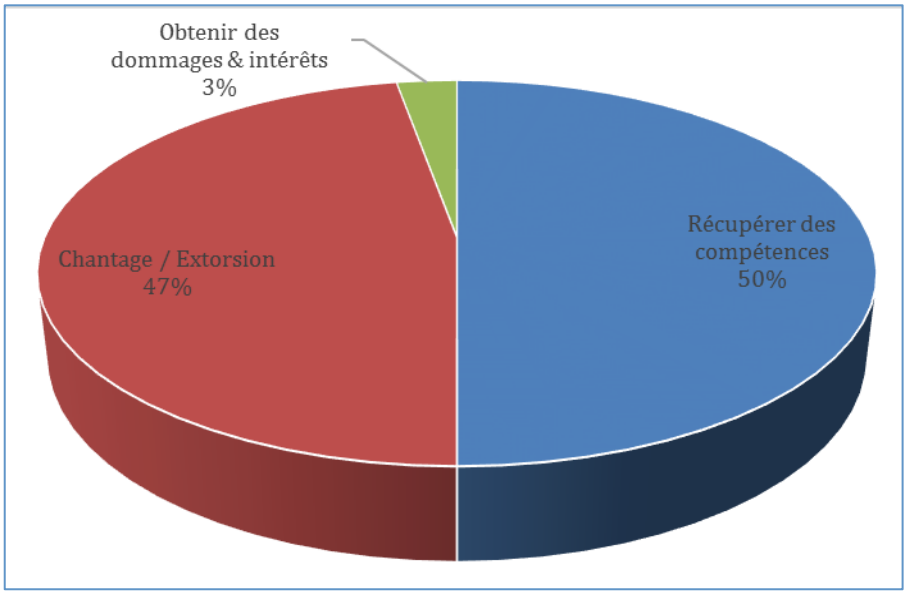
Figure 33 : Rôle de l'Attaquant

Nous constatons que le duo Pouvoir public/Concurrents représente 35% des cas traités par les Flashs Ingérence Economique. Cela s'explique par le fait que la DGSI suit essentiellement des entreprises françaises dans des secteurs stratégiques tel que la défense et qui ont une activité internationale. Ces entreprises sont susceptibles de détenir des informations sensibles et à haute valeur ajoutée pour leurs concurrents et leurs états respectifs.

Nous notons également que 30% des attaques décrites proviennent d'organisations criminelles.



4. Motivations de l'Attaquant



Comme nous l'avons vu plus haut avec la source des attaques, les motivations des attaquant se divisent en deux groupes, 50% sont motivés par la récupération d'informations ou de savoir-faire et 47% sont motivés par l'appât du gain.

5. Préméditation

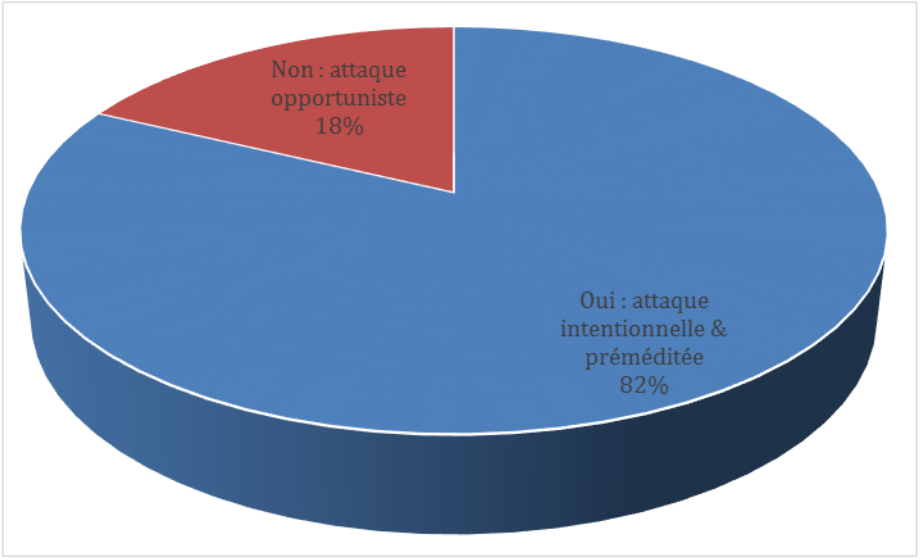


Figure 34 : Préméditation

Nous constatons une écrasante majorité d'attaques qui ont fait l'objet de préméditation, En effet étant donné leur nature, elles ont nécessité une préparation que ce soit en matière de renseignement ou d'organisation qui représente un investissement en temps.

6. Mode d'Attaque

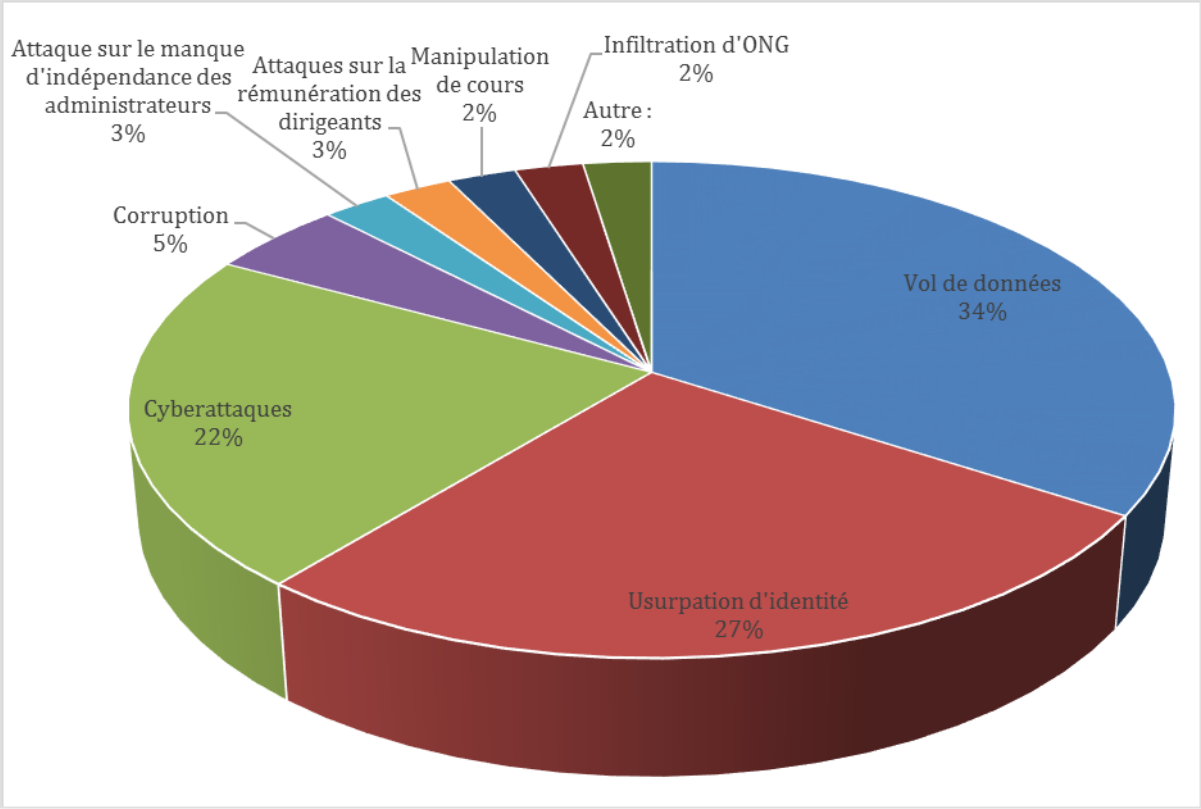


Figure 35 : Mode d'attaque

Comme nous avons pu le détailler précédemment, les cas traités dans les Flash Ingérence Economique concernent essentiellement des tentatives d'escroquerie financière et des vols d'informations. Les méthodes utilisées pour parvenir au succès de l'attaque sont très souvent liées à l'usurpation d'identité, que ce soit par téléphone ou par l'embauche de personnels.

7. Conséquences

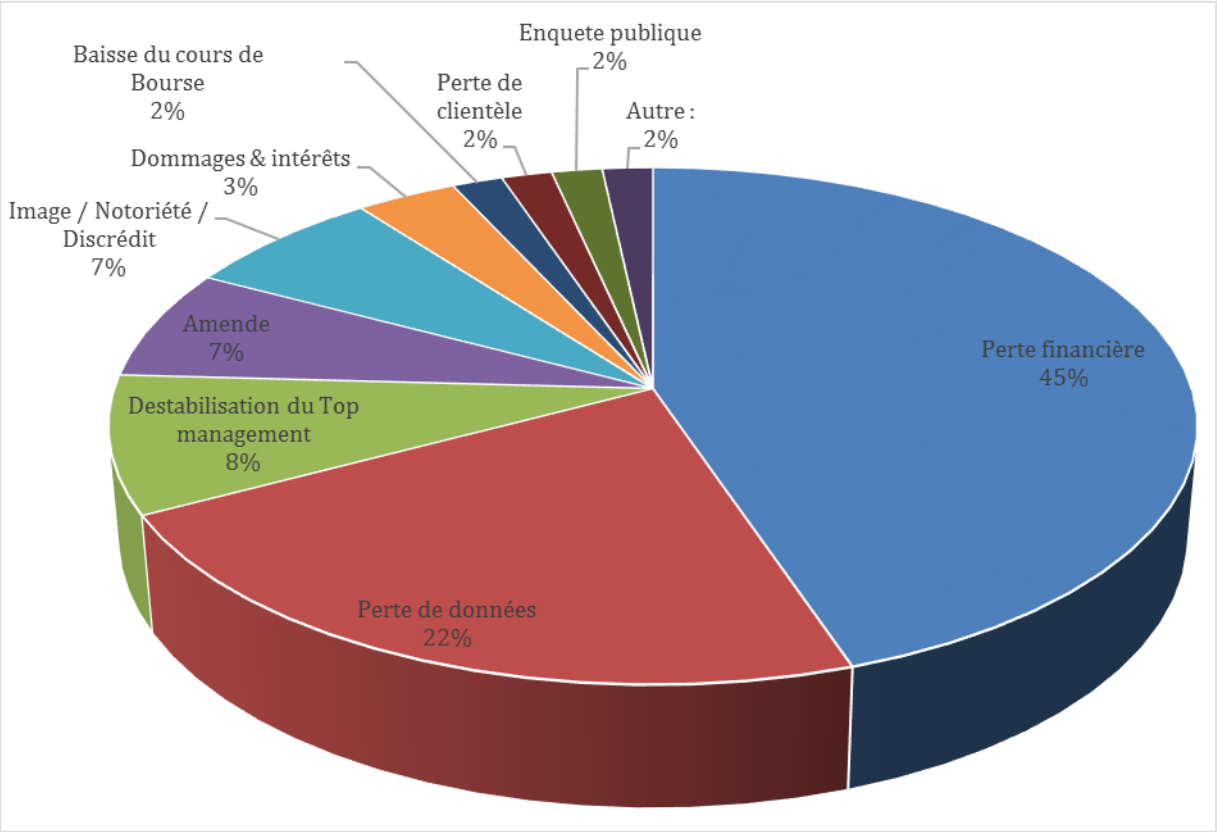


Figure 36 : Impact(s) sur la Cible

Dans la quasi-totalité des cas traités la conséquence directe est une perte financière qui peut être aggravée par une perte de données.

6. ILLUSTRATION : LES ETAS-UNIS

Dans le cadre de cette étude, nous analysons des cas d'attaques menées depuis les Etats-Unis.

Les Etats-Unis fournissent le contingent d'attaquants le plus élevé dans le panel des cas que nous avons étudiés. C'est la raison pour laquelle nous avons choisi de nous pencher plus particulièrement sur les études dans lesquelles les attaquants ont été clairement rattachés à ce pays.

Les secteurs d'activité les plus mentionnés dans les cas qui nous ont été confiés dans le cadre de cette étude se présentent comme suit :

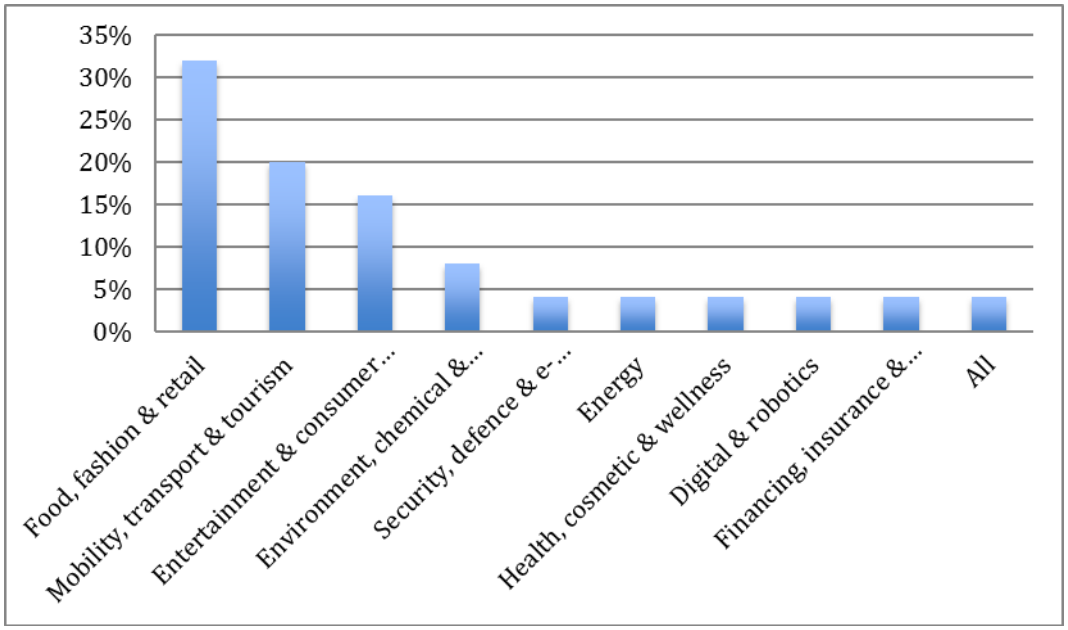


Figure 37 : Répartition des cas par secteur d'activité

Les secteurs d'activité les plus fréquemment retenus dans les cas étudiés sont ceux qui contiennent le plus grand nombre d'entreprises B to C, qu'il s'agisse d'agroalimentaire, de constructeurs automobiles ou d'entreprises du secteur des télécommunications. Nous ne sommes pas en mesure de proposer d'explications à ce sujet, si ce n'est que s'agissant de biens de consommation directement proposés aux particuliers, la communication entourant ces affaires est plus largement diffusée que pour des secteurs plus techniques comme le secteur de l'économie digitale et de la robotique ou de la banque et assurance.

La base documentaire de notre analyse peut être résumée par le graphique ci-dessous, en ce qui concerne les origines géographiques des organisations visées par les attaques américaines.

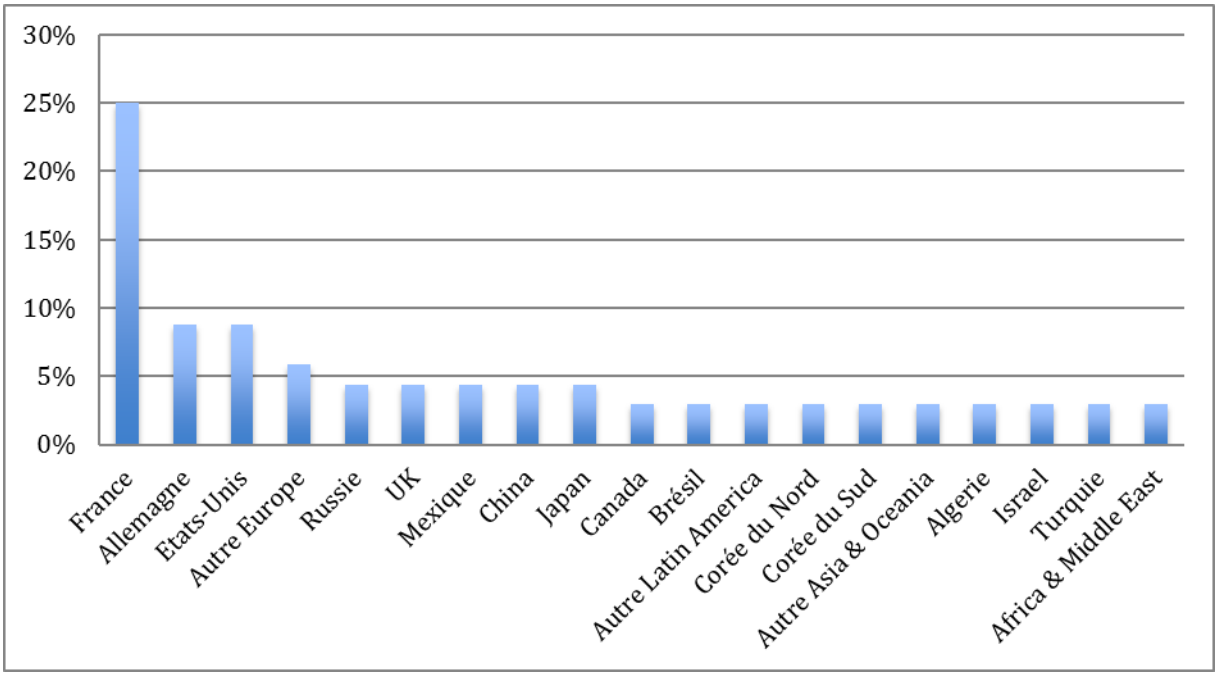


Figure 38 : Attaques états-uniennes : origine géographique des cibles

Nous retrouvons dans ce graphique ce qui peut être considéré comme une caractéristique de cette étude, à savoir qu'elle est essentiellement centrée sur la France, puisque le quart des actions menées par des organisations américaines incluses dans notre fonds documentaire ont été diligentées contre des entreprises ou des organisations françaises.

Au-delà des premières constatations purement descriptives portant sur l'origine géographique et sectorielle des cas traités, nous nous sommes posé la question du rôle des attaquants américains. Quels sont les attaquants les plus actifs aux Etats-Unis dans ces cas de déstabilisation d'entreprise ? Sont-ils les mêmes que dans l'étude générale ? Quels points d'attention peut-on mettre en avant lorsque des intervenants américains sont présents dans le « paysage » économique ?

Alors que nous travaillons sur des cas de déstabilisations sous un angle économique, nous pouvons constater que les intervenants les plus actifs sont des acteurs civils ou étatiques, dans 48 % des cas. Les concurrents apparaissent à la troisième place des

initiateurs identifiés d'attaques, suivis de plus loin par les médias et les actionnaires lorsque les entreprises sont cotées en bourse.

De façon plus détaillée, la répartition des attaquants par type de rôle peut être présentée ainsi :

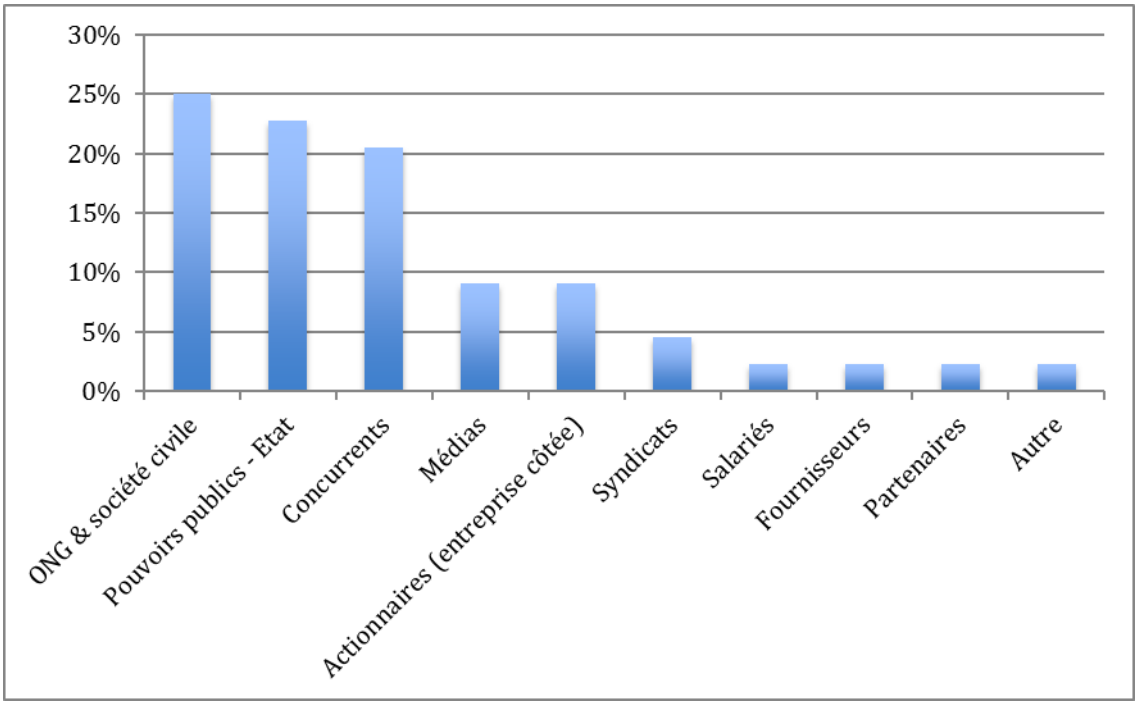


Figure 39 : Répartition des attaquants dans le panel des cas américains

Afin de déterminer s'il existe une spécificité américaine, nous avons comparé la répartition des attaquants géographique en fonction des rôles des acteurs identifiés dans les études du fond documentaire.

Nous avons exclu les cas diligentés par les organisations criminelles, parce que ces entités ne peuvent pas être rattachées à un pays particulier dans les documents étudiés. Par ailleurs, elles sont souvent transnationales.

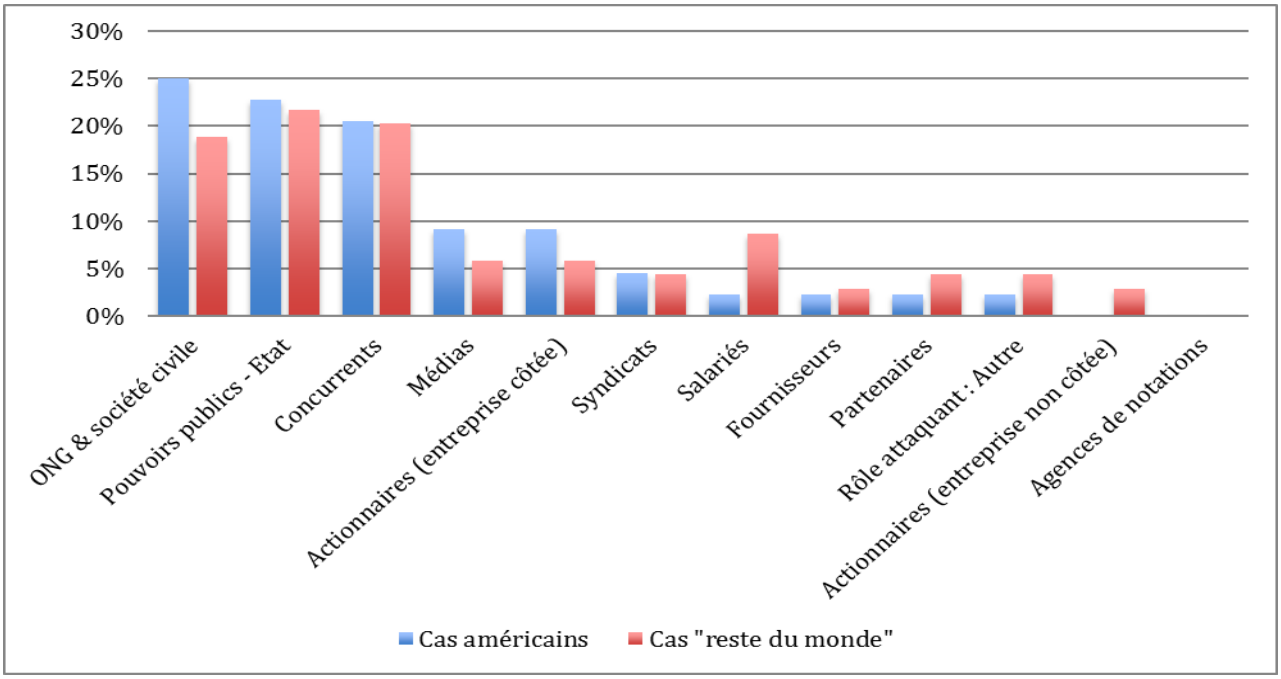


Figure 40 : Comparaison des attaquants par origine géographique (hors organisations criminelles)

Nous constatons que les principaux initiateurs d'attaques sont identiques, que les attaques soient diligentées depuis les Etats-Unis ou depuis d'autres pays. En effet, les attaques imputées aux cinq catégories principales que sont les ONG, les Pouvoirs Publics, les concurrents, les médias et les actionnaires d'entreprises cotées représentent 86 % des dossiers directement rattachés aux Etats-Unis et 72 % des dossiers imputés à des attaquants originaires du reste du monde.

Bien que ce graphique nous révèle une certaine similitude dans la répartition des acteurs, il semble mettre en évidence une préférence américaine pour l'intervention des tiers externes aux organisations, ONG et société civile d'une part et media d'autre part, pour mener les opérations d'affaiblissement économique. Notons également la part importante des actions orchestrées par les actionnaires américains de sociétés cotées par rapport aux cas attribués au « reste du monde ». Mais quel poids représentent les intervenants américains parmi chaque catégorie d'attaquants ?

Pour obtenir un éclairage sur cette question, nous avons comparé la part des cinq acteurs majeurs américains par rapport au total des opérations menées pour chaque catégorie d'attaquants.

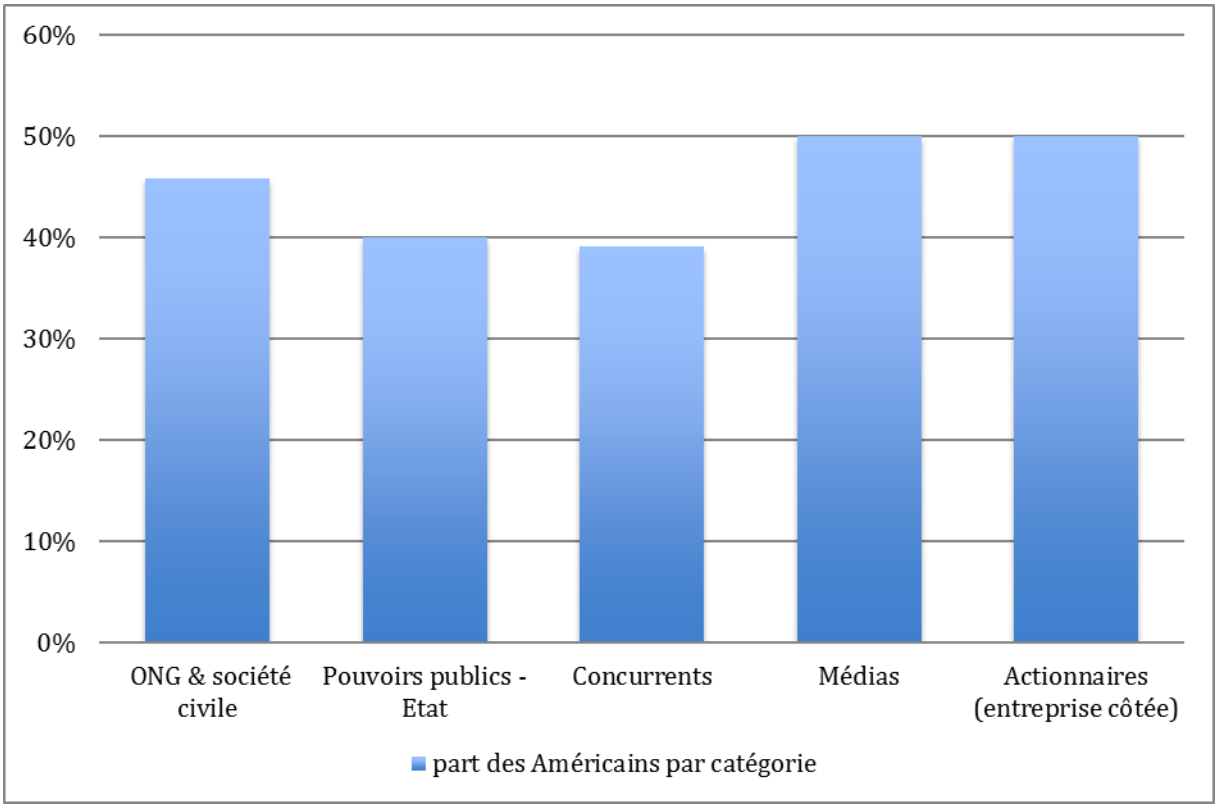


Figure 41 : Part des Américains dans les attaques menées par chaque catégorie d'acteurs

Nous pouvons constater que c'est par l'intervention des media et des actionnaires des sociétés cotées que les Américains sont les plus actifs.

En effet, il apparaît que les affaires initiées par les médias le sont pour moitié par des médias américains. Cela traduit l'importance de la communication et des médias dans la culture de ce pays, ainsi que l'utilisation qui en est faite en matière de guerre économique. Nous pouvons également noter que les ONG et la société civile américaines sont particulièrement actives en matière de déstabilisation, puisqu'elles sont à l'initiative de plus de 46 % des attaques menées par ce type de structure.

Dès ces premières constatations, il apparaît qu'à partir du moment où une structure vient en confrontation avec un acteur économique américain, soit sur le territoire américain, soit sur un autre marché, les entreprises doivent rester très vigilantes vis à vis des tiers que sont médias et les ONG. Il semble intéressant d'envisager, dès l'élaboration des orientations stratégiques, de s'adjoindre des tiers capables de se confronter à ces structures d'égal à égal pour anticiper les attaques ou les contrer le plus efficacement possible.

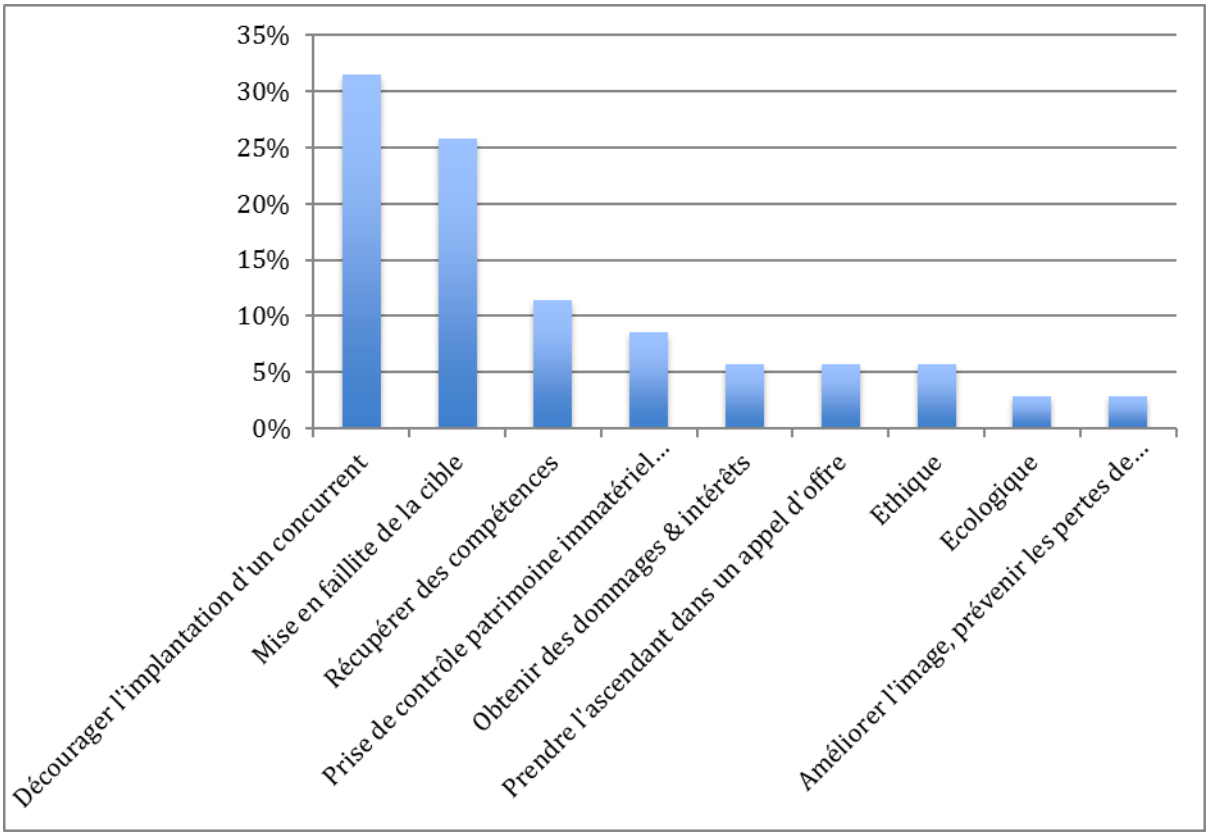


Figure 42 : Motivations des attaques

Nous avons eu l'occasion de le soulever lors de l'examen des motivations des attaquants, et pouvons le confirmer pour ce qui concerne les attaques menées par des acteurs américains : les motivations restent essentiellement économiques et financières, malgré une prédominance d'acteurs qui restent externes au business des entreprises ou organisations visées. C'est ce que confirme le schéma portant sur les motivations des attaques américaines.

Une autre tendance est confirmée s'agissant des attaques américaines, il s'agit du caractère prémédité des opérations des déstabilisations relatées dans les cas étudiés. En effet nous l'avons relevé dans 88% des cas américains ; ce qui représente un taux proche du taux général de 84 %.

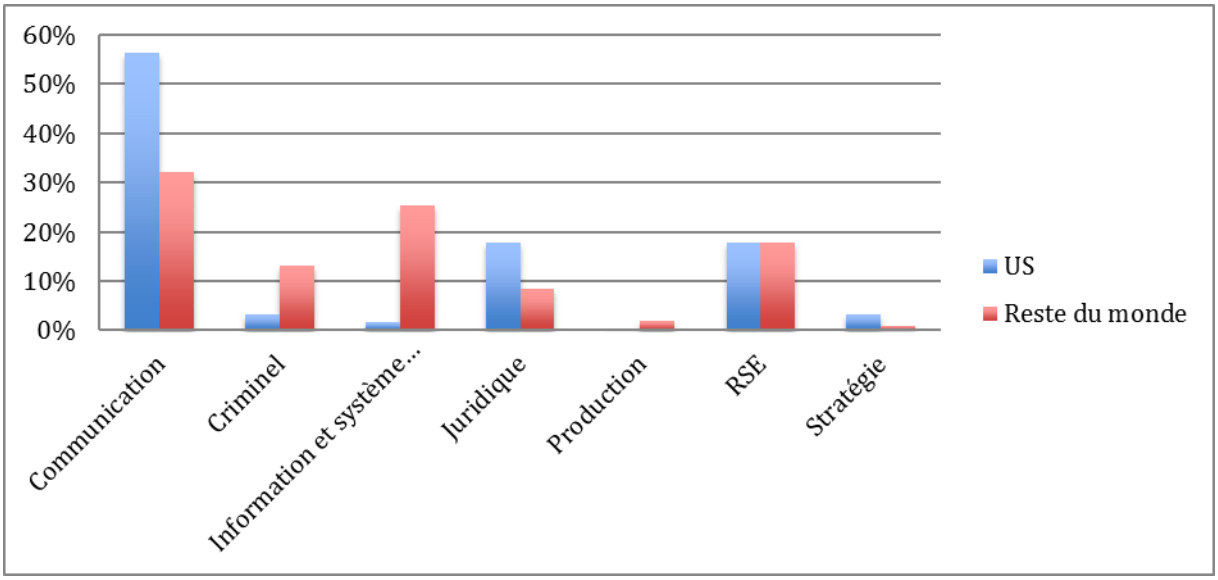


Figure 43 : Modes d'attaques

Nous avons regroupé les modes d'attaques par grandes catégories, de la même façon que nous l'avons fait pour l 'étude générale. Concernant les cas étudiés, nous avons comparé les modes d'attaques relevés sur les cas initiés par des attaquants américains et ceux diligentés par le reste du monde. Les angles d'attaques américains les plus fréquents parmi les cas qui composent le fond documentaire sont

- La communication,
- Les actions juridiques,
- L'utilisation d'arguments relevant de la responsabilité sociale et environnementale des entreprises.

Concernant les actions de déstabilisation initiées par les acteurs américains et déroulées par des opérations de communication, les modes d'actions favorisés sont ceux qui impliquent ou ont recours à des Organisations Non Gouvernementales. En effet, elles représentent à elles seules 52 % de ce type d'attaque, contre 30 % des cas diligentés par le « reste du monde ». Les opérations de dénigrement représentent le second volet des modes d'attaques de communication identifiés dans les cas que nous avons étudiés. S'agissant de publication d'articles négatifs par des bloggeurs influents ou d'opération de dénigrement dans la presse, ce sont près de 40% des attaques américaines qui sont menées par ces biais, taux très voisin des 42% constatés dans les cas attribués aux autres pays. Notons que, parmi les cas de notre fond documentaire, c'est par la plus grande fréquence des avis négatifs d'influenceurs sur les réseaux sociaux ou sur des

forums internet que les autres pays se distinguent des Etats-Unis, ces derniers favorisant les opérations de dénigrement.

Les opérations juridiques constituent le deuxième mode d'intervention américaine identifié dans notre fonds documentaire. Parmi les cas initiés par des acteurs américains, les deux modes d'actions principaux consistent à faire intervenir le législateur pour favoriser les acteurs américains au détriment de leurs concurrents, qu'il s'agisse de réglementations spécifiques au secteur d'activité ou de lois de portée plus générale. Ces interventions des pouvoirs publics représentent 45 % des cas d'utilisation du droit dans des affaires de déstabilisation diligentées par des acteurs américains contre 22% des cas attribués aux autres pays.

Enfin, nous constatons la quasi égalité de l'utilisation d'arguments relevant de la RSE que les cas soient imputés à des attaquants américains ou non. Cela peut être lié à la composition de notre fonds documentaire, très centré sur des organisations occidentales.

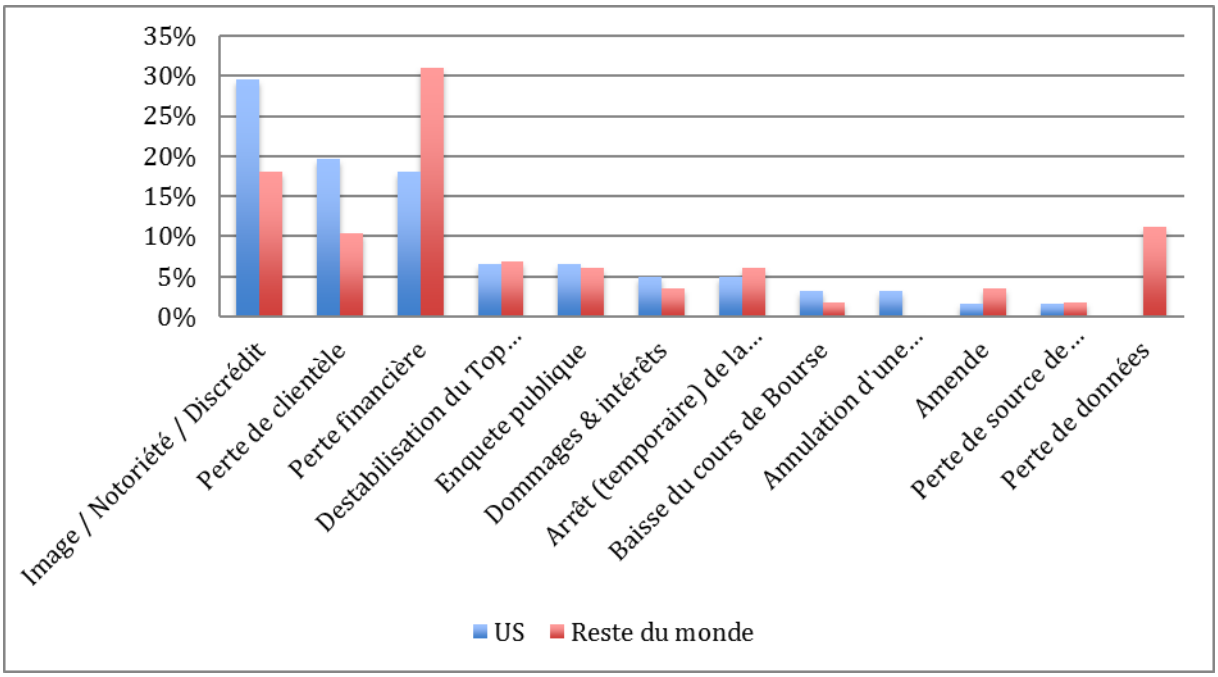


Figure 44 : Impact des attaques sur les cibles

Le graphique ci-dessus présente l'impact des attaques sur les structures visées selon l'origine géographique des attaquants. Trois conséquences se détachent comme les

principaux impacts, représentant 67% des cas américains et 59 % des cas attribués à des acteurs hors des Etats-Unis :

- les conséquences sur l'image
- la perte de clientèle
- les pertes financières.

Cohérent avec les modes d'attaques de type « communication » et des intervenants des media très actifs dans les cas étudiés, les conséquences principales portent sur l'image et la notoriété des structures, particulièrement dans le cas des attaques américaines.

La perte de clientèle est ensuite identifiée par les auteurs des études comprises dans le périmètre de notre travail comme l'une des conséquences majeures des attaques menées depuis les Etats-Unis, la perte financière directe, c'est-à-dire ayant un impact immédiat sur les états financiers, n'arrivant qu'en troisième position.

D'après les cas qui constituent notre fonds documentaire, les attaques initiées par des acteurs américains ont des conséquences plus étalées dans le temps. En effet, le discrédit et les atteintes à l'image ainsi que la perte de clientèle peuvent avoir des effets pendant de nombreuses années.

7. CONCLUSION

Les cas analysés dans cette étude permettent de mettre en exergue des stratégies de déstabilisations différentes selon les secteurs d'activités. Les moyens mis en œuvre, les acteurs, les finalités des cas de déstabilisations diffèrent donc. Une approche sectorielle prend tout son sens et nécessite d'être développée par une étude plus exhaustive afin de tirer des conclusions plus précises.

L'étude devra aussi diversifier les secteurs, tels que chimie, ou la métallurgie, car elle a porté sur un tiers des secteurs d'activités généralement considérés.

Autre constat, la prééminence des pouvoirs publics dans le jeu de la déstabilisation dans la préservation des intérêts politiques et économiques des états.
Cette étude ayant été réalisée sous le prisme Franco-Français, elle ne représente pas la réalité mondiale des cas de déstabilisations. Elle permet cependant la mise en avant de certains acteurs importants.
Le poids de la Chine, acteur émergent de l'économie mondiale ne transparait pas dans cette étude. Elle concentre cependant un nombre important d'attaques dans le domaine des nouvelles technologies. (Huawei, ZTE, etc.).
La guerre économique que se livrent de nos jours les états est désormais affirmée, revendiquée et assumée. Les mécanismes employés sont violents et ne cherchent plus à se dissimuler :

- Politiques douanières
- Restriction d'accès au marché
- Guerre Militaire

En annexe de cette conclusion, les étudiants ayant participé à cette étude préconisent de poursuivre ce travail et d'enrichir la base de cas afin qu'elle soit alimentée en permanence :

- De mettre à jour la base à chaque nouveau cas
- Que la base soit ouverte aux anciens pour compléter la base
- De mettre en place un outil plus structuré avec des filtres

- D’analyser l’ensemble des secteurs d’activités notamment ceux en dehors de la présente étude.

EGE Ecole de Guerre Economique

SURVEILLER. ANALYSER. PROTEGER. INFLUENCE.

196, rue de Grenelle, 75007 Paris / +33 1 45 51 00 02 / contact@ege.fr / www.ege.fr