Méthodologie d'analyse d'attaques informationnelles à base de cas réels

Danielle Kaminsky

Chercheur en criminalité informatique

1 Introduction

La plupart des attaques informationnelles conduites sur Internet ou amplifiées sur le réseau sont faciles et peuvent être violentes. Attaques mixtes, elles conjuguent utilisation des systèmes d'information et opérations psychologiques destinées à servir une stratégie de contrôle ou de domination. L'angle qui nous intéresse ici est la menace contre la sécurité économique des entreprises. L'usage des moyens informatiques pour affaiblir ou entraver l'activité des entreprises comporte une double menace : comme s'il ne leur suffisait pas d'avoir à se prémunir des virus, du piratage, de l'espionnage, la plupart des entreprises françaises subissent des attaques informationnelles sans être capables de comprendre à temps qu'elles sont sous attaque et quels sont les modes opératoires.

Les cas réels d'attaques informationnelles décrits ici ont été choisis sur les critères suivants :

1. L'attaque se sert majoritairement des systèmes d'information : Internet, Usenet, messageries électroniques, listes de discussion.
2. L'attaque est commise à visage masqué, elle nécessite donc une investigation pour être appréhendée.
3. Les cas choisis ont fait l'objet d'informations publiées dans la presse, raison pour laquelle les noms des interessés sont mentionnés.

L'étude des cas présente une méthodologie s'appuyant sur une grille de paramètres précis pour aider à détecter la menace, caractériser les attaquants, déterminer l'origine et comprendre la nature et l'ampleur de l'attaque afin d'améliorer la connaissance et la protection contre ces risques.

L'attaque informationnelleest considérée ici comme étant tout un acte délibéré qui utilise l'information pour générer une mauvaise perception, déstabiliser, discréditer, démoraliser, nuire.

Les cibles peuvent aussi bien être des individus, des entreprises, des produits, des programmes, des projets....

Les auteurs des attaques informationnelles déstabilisatrices d'entreprises ou d'organismes peuvent aussi bien être des particuliers agissant par colère, vengeance, frustration, ou autre motivation personnelle, que des individus agissant au service d'intérêts concurrents ou adverses.

- **Cas 1** : Attaque informationnelle contre un article scientifique.
- **Cas 2** : Attaque informationnelle contre un groupe pharmaceutique.

2 Cas : Décrédibilisation d'un article scientifique

En novembre 2001, le magazine scientifique *Nature* publie un article de deux chercheurs de l'Université de Berkeley en Californie, Ignacio Chapela et David Quist. Leur étude montre que du maïs mexicain a été contaminé par du pollen de plante génétiquement modifiée, à distance. Un article publié dans la revue Nature apporte une valeur de crédibilité. Pourtant, en mars 2002, *Nature* indique que l'article n'aurait jamais dû être publié.

2.1 Que s'est-il passé ?

Le journal britannique The Guardian va le raconter. Dans son article titré " *The Fake Persuaders* ", publié le 14 mai 2002, Georges Monbiot soutient qu'une opération masquée de décrédibilisation a été orchestrée contre les deux chercheurs, parce qu'ils auraient dérangé les intérêts d'une grande firme spécialisée dans les OGM. L'article du Guardian se fonde sur le travail d'un militant et d'un autre journaliste, qui concluent qu'une société de relations publiques spécialisée dans le lobbying Internet - The Bivings Group - aurait envoyé dans un espace de discussion de faux internautes, pour distiller le doute sur l'étude des deux chercheurs californiens.

L'article du Guardian raconte que le jour-même de la publication dans *Nature*, des messages ont commencé à apparaître sur le site d'AgbioWorld, une fondation spécialisée en biotechnologies, qui propose des espaces de discussion lus par des milliers de scientifiques de par le monde. Il rapporte que le premier message émanait d'une " Mary Murphy ", bientôt suivie par " Andura Smetacek ". L'une dit que l'un des auteurs n'est pas ce qu'on pourrait appeler un auteur objectif. L'autre que l'article n'a pas été relu par une tierce partie, et que son auteur est avant tout un activiste. Le lendemain, un autre message de " Andura Smetacek " demande : " Combien d'argent Chapela prend pour ses communications, le remboursement de ses frais de transport, et autres donations....pour son aide à un marketing trompeur basé sur la peur ? ". Suivent d'autres interrogations semant le doute et bientôt, des centaines de messages font boule de neige et amplifient ce doute. AgbioWorld lance une pétition qui souligne les défauts de l'article.

Lorsque Nature indique que la recherche des deux auteurs de l'Université de Berkeley n'aurait jamais dû être publiée, le journal The Guardian monte au créneau et dénonce l'opération. Les enquêteurs se sont intéressés au début de la campagne de décrédibilisation.

2.2 Qui sont les personnes à l'origine du mouvement ? Agissent-elles pour des motifs personnels ou au service d'intérêts commerciaux ?

Qui sont " Mary Murphy " et " Andura Smetacek " ? Les deux proclament être citoyennes ordinaires, sans aucun lien commercial. Une recherche sur les messages les plus anciens de " Mary Murphy ", avec la même adresse à un compte

Hotmail, révèle des traces techniques : `bw6.bivwood.com`. Or, Bivwood.com appartient à Bivings Woodell. Une société qui fait partie du groupe Bivings.

Lorsqu'il questionne " Mary Murphy " par email, le journaliste du Guardian se voit répondre qu'elle n'a aucun lien avec un industriel, mais il n'obtient aucune réponse à sa question de savoir si Mary Murphy est son vrai nom ou pas. Il relève alors un détail intéressant : son " interlocutrice " lui dit qu'elle voit dans ses articles qu'il a déjà un partie pris sur les biotechnologies. Or, explique Georges Mondiot, il n'avait pas du tout parlé de biotechnologie dans son email, mais annoncé qu'il faisait une recherche sur le lobbying sur Internet.

Une recherche sur l'autre posteur de messages, " Andura Smetacek " conduit à un autre lien avec la même entreprise, faisant partie du même groupe Bivings.

Sur le site web de la firme de relations publiques spécialisée dans le lobbying Internet, le journaliste remarque un texte titré : " *Viral Marketing : How to infect the World* ", qui dit : " *Il y a certaines campagnes où il n'est pas souhaitable, voire désastreux, que le public sache que votre entreprise est directement impliquée* ". Il remarque aussi un message de félicitations d'un cadre d'une grande firme spécialisée dans les OGM pour " *l'admirable travail* " réalisé par la firme de relations publiques.

L'article du Guardian dénonce les pratiques clandestines d'influence attribuées à la firme de relations publiques et y consacre un deuxième article, publié quinze jours plus tard, titré : " *Corporate Phantoms* ".

Le Président de Bivings Group va démentir que sa firme aurait joué un rôle dans l'opération de sape à visage masqué contre l'article de Nature. Dans une lettre adressée au Guardian, il assure que " Mary Murphy " et " Andura Smetacek " ne sont ni employées ni prestataires de sa société, et qu'il ne les connaît ni l'une ni l'autre.

Peu de temps après, dans une émission de la BBC, un cadre de Bivings Group aurait répondu que l'un des emails en cause avait été envoyé par " *quelqu'un travaillant pour Bivings* " ou des " *clients utilisant nos services* ".

Dans son deuxième article titré " *Corporate Phantoms* ", Georges Monbiot poursuit ses révélations sur cette affaire. Il écrit qu'alors qu'il écrivait son précédent article (" The Fake Persuaders "), Bivings Group lui avait envoyé un email démentant avoir un quelconque rapport avec les faux correspondants " Mary Murphy " et " Andura Smetacek " à l'origine de la campagne contre l'article de Nature dans l'espace de discussion scientifique sur les biotechnologies.

Puis le journaliste ajoute : " *La semaine dernière, j'ai vérifié les propriétés techniques de l'email. Elles contenaient :* `bw6.bivwood.com`. *Le message provenait du même ordinateur que celui utilisé par " Mary Murphy ". Une nouvelle recherche effectuée par le militant Jonathan Matthews s'avère avoir démasqué les faux persuadeurs : " Mary Murphy " conduit à un webdesigner de Bivings, écrivant aussi bien depuis le bureau que depuis son domicile à Hyattsville dans le Maryland, tandis que " Andura Smetacek " se révèle être le chef marketing Internet de la société.* "

2.3 Méthodologie d'analyse

Nous n'allons pas nous attacher dans cet exemple à déterminer qui a raison ou tort sur le fond, mais d'étudier ce qui se passe, et selon quel mode opératoire.

Fait déclencheur La publication de l'article dans la revue Nature. Le fait déclencheur est connu au moment de l'attaque. Il est mentionné par les attaquants eux-mêmes.

Auteurs-perpétrants de l'attaque informationnelle Deux personnes. Agissant à visage masqué. Ne sont pas chercheurs scientifiques. Se révèlent être des émissaires (agents) par l'investigation. Reliés à une entreprise avec intérêts commerciaux soutenant les OGM. Intérêts en opposition avec le résultat de l'étude publiée par les chercheurs.

Lieu où s'effectue le lancement de l'attaque C'est un lieu choisi : un espace de discussion sur Internet spécialisé dans les biotechnologies suivi par de nombreux scientifiques de plusieurs pays concernés par le sujet. Il appartient à une fondation. La caractéristique de cette fondation est de soutenir les biotechnologies.

Caractéristiques du lieu choisi : espace public à forte visibilité, portée mondiale, fréquenté par des scientifiques.

Assistance choisie pour l'attaque Des scientifiques. Tout comme les chercheurs auteurs de l'article publié dans Nature.

Contenu de l'attaque-axes thématiques Les messages injectés par les deux personnes sèment le doute sur la crédibilité de l'étude par la mise en cause de ses auteurs.

Le fond de l'étude est sapé par une attaque contre les hommes (attaque " ad hominem "). L'objectivité des auteurs de l'étude est explicitement mise en cause. Bien plus, les auteurs de l'article incriminés sont désignés comme des " activistes ". C'est le thème central de l'attaque.

Le troisième argument disant que l'étude n'a pas été relue par une tierce partie contribue à renforcer l'attaque sur le thème du manque d'objectivité des chercheurs. Sans même que l'on sache si la relecture a eu lieu ou pas, et si elle aurait conduit à écarter le texte de l'article, le fait d'évoquer l'absence de tierce partie fait porter l'attention sur un manque.

Quatrième argument d'attaque : l'argent. Les auteurs de l'étude gagnent de l'argent qui alimente des intérêts.

Les intérêts en question ne sont pas nommés directement, mais sont caractérisés par le mot " marketing " qui évoque clairement une stratégie, un plan de communication. Implicitement, c'est la connotation de manipulation qui transparait.

L'expression : “ basé sur la peur ” choisie pour qualifier ce “ marketing ” induit également la notion de plan, et en même temps colore ce plan de manière à provoquer une méfiance de la part des lecteurs. Le qualificatif “ trompeur ” est la pièce maîtresse de l'édifice. L'expression entière “ marketing trompeur basé sur la peur ” effrite et supprime d'un coup la valeur de recherche de l'étude pour lui substituer celle d'opération de manipulation.

Intensité. L'attaque est conduite en crescendo, et en quelques paliers seulement. Le passage entre les notions de manque d'objectivité à celui d'opération calculée et trompeuse s'effectue rapidement, en quelques phrases.

Amplification L'effet boule de neige est assuré dès lors que plusieurs membres de la liste de discussion ajoutent leur contribution et amplifient le doute. Le point étape de l'attaque est la pétition, suivie du point culminant marquant la réussite de celle-ci : la mise en cause par *Nature* de l'article que la revue avait elle-même choisi de publier.

Temps Les deux intervenants qui sèment le doute restent peu de temps dans l'espace de discussion. Après avoir enclenché la mécanique du doute, ils s'éclipsent et laissent les participants se charger de la dissémination et de l'amplification.

Première phase : le temps de leur intervention, court.

Deuxième phase : la machine est lancée et dans cette phase de temps, plus longue, ce sont les autres qui vont alimenter la machine.

Troisième phase : la pétition.

Quatrième phase : l'obtention du mea culpa de la revue.

C'est le couperet. De la publication de l'article dans Nature au désaveu par celle-ci, il se sera écoulé seulement 4 mois.

Anomalies et erreurs commises Plusieurs anomalies permettent de déceler la présence d'une attaque informationnelle.

L'intervention à visage masqué. Les traces techniques dans les en-têtes de messages relient les auteurs de l'attaque à une firme soutenant les intérêts commerciaux opposés. Les traces techniques montrant que les deux intervenants ont émis des messages à partir du même ordinateur.

Le fait que, questionnée par le journaliste du Guardian, l'une des interlocutrices lui reproche un parti pris contre les biotechnologies. Or, explique Georges Mondiot, il n'avait pas du tout parlé de biotechnologie dans son email, mais annoncé qu'il faisait une recherche sur le lobbying sur Internet.

D'autres interventions de l'un des acteurs renforcent l'hypothèse de l'attaque informationnelle organisée professionnellement.

Le journaliste Georges Monbiot rapporte que “ Andura Smetacek ” a déjà émis d'autres messages, faisant à plusieurs reprises la promotion d'un “ the Center For Food and Agricultural Research. ”, un site web dont Georges Monbiot précise qu'il est enregistré au nom d'un cadre de l'entreprise Bivings Woodell.

Contexte de l'attaque La culture de plantes transgéniques n'est pas autorisée au Mexique à l'époque des faits. La culture de plantes transgéniques suscite des oppositions dans plusieurs pays.

Forme de l'attaque Il ne s'agit pas d'une attaque frontale, mais d'une attaque indirecte. Les attaquants ne s'adressent pas directement aux chercheurs auteurs de l'article, mais à un public tiers. Il leur est dévolu à leur insu le rôle d'amplifier l'attaque. De surcroit, les attaquants agissent à visage masqué. Sans investigation, ils auraient pu ne pas être reliés à des professionnels soutenant des intérêts commerciaux adverses. L'attaque est perpétrée en public, elle vise une portée mondiale.

Impact souhaité Mise en doute de l'étude auprès d'autres chercheurs du domaine concerné.

Impact effectif Discrédit de l'étude auprès d'autres chercheurs du domaine concerné. Discrédit auprès de la revue scientifique Nature.

Impact potentiel supplémentaire Discrédit potentiel de l'Université où travaillent les chercheurs. Difficultés éventuelles de financement de leurs prochaines recherches.

3 Dénigrement d'un groupe pharmaceutique

Cette affaire a fait l'objet d'une décision de Justice en France, en novembre 2003.

Le groupe pharmaceutique Smith & Nephew a été bombardé pendant presque deux ans de messages électroniques dénigrants. Les messages étaient adressés à plusieurs dizaines de ses dirigeants et salariés, en France et dans plusieurs pays du monde. L'attaque débute par une e-carte envoyée depuis le site web d'une municipalité française, par l'intermédiaire de la rubrique " envoyez une e-card à un ami ". La carte est accompagnée d'un message au contenu particulièrement dur, puisqu'il affirme que les produits du groupe pharmaceutique sont défectueux ou mortels, ses dirigeants corrompus.

Plusieurs milliers de messages sont envoyés aux salariés de l'entreprise. Leur nombre est si élevé qu'il provoque une saturation .

Mais ces messages ne sont pas seulement envoyés à des salariés de la firme. Des partenaires commerciaux et financiers, des concurrents et des organes de presse en reçoivent également.

3.1 Méthodologie d'analyse de l'attaque

Fait déclencheur Non connu au moment de l'attaque.

Destinataires de l'attaque Les destinataires des messages sont spécifiés. L'attaque est portée directement sur plusieurs cercles de l'entreprise visée.

Public interne à l'entreprise : Il s'agit de salariés et dirigeants du groupe pharmaceutique visé par l'attaque.

Public interne élargi : les salariés du groupe à l'étranger. Ces destinataires sont sélectionnés et nommément précisés par leur adresse email.

Public externe : les partenaires fonctionnels de l'entreprise, commerciaux et interlocuteurs financiers. Ces destinataires appartiennent au second cercle de l'entreprise, les interlocuteurs fonctionnels, ils sont également sélectionnés et nommément désignés par leur adresse email destinataire.

Public externe : Un autre cercle est visé par l'attaque : les concurrents, auxquels des messages sont également envoyés.

Public externe plus large : les médias. Ils sont également externes, et ont la possibilité de démultiplier la résonnance de l'attaque s'ils la relaient.

Impact souhaité Il est énorme, puisque l'attaque s'adresse à tous les cercles importants : le coeur de l'entreprise, ses interlocuteurs fonctionnels, ses concurrents et les médias. A travers les médias, c'est l'impact auprès des clients et des consommateurs qui est recherché.

Ces cercles internes, fonctionnels, concurrentiels et médiatiques sont capables de briser le lien de confiance qui unit l'entreprise à sa clientèle et nuire à la prospérité, et même à la pérennité de l'entreprise.

Caractéristique de l'attaque à ce niveau : il s'agit d'une attaque méthodique et acharnée. Aucun type de destinataire n'est écarté, ce qui donne le maximum de chances à l'attaque d'aboutir à l'impact souhaité. Par ailleurs, l'attaque est perpétrée sur une longue durée (presque deux ans).

Il s'agit d'une attaque très grave, l'impact souhaité est de nature à voire s'effondrer l'image de l'entreprise et son activité. L'attaque représente donc un très haut degré de risque pour l'entreprise.

Durée de l'attaque Pour l'entreprise visée par une telle attaque, il est vital d'identifier le plus rapidement possible l'auteur.

Pour cela, il faut d'abord qu'elle sache qu'elle est sous attaque. Dans ce cas précis, tout dépend de la rapidité avec laquelle les destinataires internes des emails vont remonter l'information auprès de la direction et conserver les éléments utiles à l'enquête.

Cette attaque aura duré presque deux ans.

Identification de l'auteur de l'attaque : étude des éléments apparents et du mode opératoire dans l'envoi des messages, analyse technique, analyse de contenu, précédents (cas similaires) Qui envoie ces messages ? L'attaque procure les signes apparents d'être commise par plusieurs attaquants. Plus précisément, l'adresse d'expéditeur des messages " indique " que ces messages proviennent de personnes appartenant au groupe pharmaceutique.

Vérifications techniques : les messages électroniques proviennent-ils de l'entreprise ? En l'occurence, non. Ils ne proviennent pas de l'entreprise. L'analyse technique permet de montrer que les adresses emails d'expéditeur ont été usurpées.

En réalité, ces millliers de messages ne proviennent que d'un émetteur unique.

Le mode opératoire choisi est toujours le même : les messages sont envoyés par l'intermédiaire de sites web avec une rubrique qui permet de transférer un contenu. L'attaque a débuté par une e-carte envoyée depuis le site web d'une municipalité française, par l'intermédiaire de la rubrique " envoyez une e-card à un ami ".

L'attaque procure des signes apparents d'être commise par plusieurs sources depuis plusieurs pays : elle est perpétrée via des sites français et étrangers (médicaux, financiers, d'information), environ 80 sites différents, situés dans le monde entier.

Il pourrait s'agir d'une attaque coordonnée en provenance de multiples sources.

Or tous les sites web utilisés comportent une rubrique " envoyez une e-card " ou " envoyez cet article à un ami ".

Le champ " expéditeur " des emails est rempli avec des adresses emails choisies , le plus souvent celles de dirigeants du groupe Smith & Nephew. Le champ " destinataires " comporte des dizaines d'adresses, appartenant aussi bien à des personnes du groupe, que des partenaires ou des concurrents du groupe, des analystes financiers, des journalistes...

Ce qui suppose une connaissance très précise des noms des salariés du groupe, ainsi que ceux de son environnement, notamment ses interlocuteurs fonctionnels.

Les messages sont envoyés manuellement à plusieurs dizaines de destinataires à la fois. A un moment, l'attaquant trouve un moyen pour automatiser ses envois, et en augmenter la fréquence d'envoi, atteignant à un moment plus de 10.000 messages par heure. Ce qui aura pour effet de saturer la messagerie électronique des destinataires. En tout, 700.000 messages auront été envoyés au groupe pharmaceutique sur une durée de presque deux ans. Sans compter le nombre de messages envoyés à des interlocuteurs extérieurs à l'entreprise, nombre qui n'est toujours pas connu.

Ce très grand nombre de message et leur fréquence d'envoi sont des signes d'acharnement. La durée de l'attaque l'indique également. Ainsi que le temps consacré à l'attaque (dates et heures).

Mais surtout, l'analyse de contenu des messages dénigrants comporte une thématique qui est constamment très dure. Elle dénote une animosité et une hostilité particulièrement forte, de nature à indiquer une charge émotionnelle. Donc un rapport personnel avec l'entreprise.

Par ailleurs, les messages s'adressent à de multiples destinataires situés à l'étranger, or l'analyse de contenu peut mettre en évidence qu'il y a eu recours à des logiciels de traduction automatique, qui serviront à correspondre dans neuf langues différentes.

Enquête : répertorier systématiquement chaque message reçu à l'intérieur du groupe pharmaceutique : date, heure, adresse d'expédition falsifiée, destinataires

connus, type de contenu dénigrant, site utilisé pour l'envoi. Ce travail permet d'identifier les fréquences et sources d'envoi et d'interroger les sites utilisés par l'attaquant pour leur demander l'adresse IP de l'ordinateur qui s'est connecté à leur site avec cette adresse.

Dans ce cas, plusieurs centaines de demandes par e-mail ont été effectuées, qui se sont soldées à de nombreuses reprises par des fins de non recevoir (par exemple, les sites web étrangers demandent une réquisition judiciaire exécutoire dans leur pays).

Mais une trentaine de réponses sont obtenues. Les adresses IP sont différentes, mais elles correspondent toutes à un accès à Internet en ADSL, via un compte Wanadoo situé à Toulouse.

L'entreprise dépose plainte et les services de l'OCLCTIC vérifient et confirment les résultats des investigations menées, puis s'adressent à Wanadoo pour obtenir l'identification de l'auteur.

Celui-ci se révèle être un ancien salarié du groupe dans la région toulousaine, licencié quelques années auparavant pour faute grave.

Précédents : l'homme était déjà poursuivi par le groupe pharmaceutique pour faux en écriture privée dans une autre affaire, pour avoir envoyé des fax préjudiciables au groupe en France. L'auteur utilisait un mode opératoire presque similaire : falsification du numéro d'envoi des fax pour faire croire que l'entreprise en aurait été l'expéditeur, thématique sur le thème de la corruption....

Intérêts servis par l'attaque Dans ce cas, l'attaque informationnelle est forte, et aurait pu faire croire à une attaque menée par un concurrent. Or, manifestement, l'auteur de l'attaque a agi pour des motifs personnels de colère-vengeance.

4 Méthodologie d'analyse-Grille

Les paramètres ci-dessous permettent de comprendre le tableau d'une situation. Ils ne sont pas exhaustifs et tous ne trouvent pas nécessairement de réponse immédiate lors du travail d'investigation sur une attaque informationnelle, comme nous l'avons vu dans les exemples décrits précédemment. Mais ils procurent une grille d'analyse réellement opérationnelle :

1. Cible de l'attaque.
2. Domaine d'activité de la cible.
3. Contexte de la cible.
4. Evénement déclencheur - Evènement prétexte.
5. Contexte de l'attaque.
6. Thématique de l'attaque : thème choisi, précédents sur ce thème ou sur ces thèmes, teneur, tonalité, intensité, èvolution de la thématique.
7. Espace : lieu de lancement de l'attaque, ampleur, autres lieux, signification des lieux - Raisons du choix des lieux : public et impact souhaités.

8. Dissémination : recherche de relais et caisses de résonnance : public et impact souhaités, recherche de contact avec les médias, réinjection, attitude vis à vis de la réinjection.
9. Temps : moment du lancement de l'attaque, attaque éclair ou attaque distillée, amplitude, durée de l'attaque dans le temps, temps passé par jour, entretien de l'attaque, organisation dans le temps, rythme, pics et pauses, relances, réactivation de l'attaque.
10. Moyens techniques employés.
11. Acteur principal : identification de l'auteur, acteur unique, personne identifiée, historique, personne sous pseudonyme(s) (masque), comment l'individu se présente, quelles idées il défend, précautions techniques, réactions face à la contradiction.
12. Agents - Renforts - Assistants : personnes identifiées, personnes sous pseudonymes, historique, comment ils se présentent, nombre, organisation : qui intervient quand et sur quel sujet, en réponse à qui - Précautions techniques, réaction face à la contradiction. Caractéristiques et Préférences des agents
13. Réseau de liens.
14. Origine de l'attaque : qui a intérêt à lancer l'attaque, qui peut être derrière, commanditaire.
15. Intérêts servis par l'attaque : personnels (jalousie, colère, vengeance, frustration, cupidité...), protestataires (opinion), èconomiques et financiers (concurrence).

Références

1. Ignacio Chapela et David Quist, Transgenic DNA introgressed into traditional maize landraces in Oaxaca, Mexico, *Nature*, Vol. 414, pp. 541–543, 2001. `http://www.cnr.berkeley.edu/chapelalab/Research/Chapela_Research.htm` (Cas 1). bibitemkk2 Georges Monbiot, The Fake Persuaders, *The Guardian*, 14 mai 2002. `http://www.guardian.co.uk/comment/story/0,3604,715153,00.html` (Cas 1).
2. Georges Monbiot, The Corporate Phantoms, *The Guardian*, 29 mai 2002, `http://www.guardian.co.uk/comment/story/0,3604,723899,00.html` (Cas 1).
3. Danielle Kaminsky, Méthodologie : Fiabilité de l'information : révélations, influences, mensonges...retour à la case départ, *Netsources* vol. 46, Septembre-Octobre 2003 (Cas 1).
4. `http://www.legalis.net/jnet/2003/actualite_11_2003.htm` (Cas 2)
5. `http://www.legalis.net/jnet/decisions/diffamation/tgi_mans_071103.pdf` (Cas 2)