Brandy Faustine
Eveillard Hubert
Francez Romain
Laurent Antoine
Marchal Morgan

QUELS SONT LES IMPACTS DE LA SOCIETE DE L'INFORMATION SUR LES RAPPORTS DE FORCE ECONOMIQUES ?

Sous la direction de Christian HARBULOT

Le 13 décembre 2012

Ecole de Guerre Economique
PXVI

Sommaire

« Celui qui gagnera la prochaine guerre n'est pas celui qui aura la plus grosse bombe, mais celui qui racontera la meilleure histoire. », David Ronfeldt[1]

[1] J. Arquilla, D. Ronfeldt, *The Emergence of Noopolitik: towards an American information strategy*, The rand corporation edition.

Introduction

Quelque soit l'endroit où nous sommes sur la planète, nous tendons à avoir accès aux même informations, aux même médias, aux même outils. Ce qui est appelé société de l'information peut être défini comme un environnement dans lequel les nouvelles technologies de l'information et de la communication (NTIC) permettent la production, la transmission et le stockage d'informations dématérialisées. Son émergence au début des années 90, notamment grâce à internet a changé le rapport des individus à l'information.

Dans ce monde numérique, la notion de frontière, d'aire géographique s'est vue transformée au regard de l'immédiateté de leur transmission et de leur accessibilité accrue. De par le spectre géographique et la population qu'elle recouvre, la société de l'information, est devenue un nouveau lieu d'influence et de pouvoir. Cette réalité fait d'elle aujourd'hui un nouveau terrain d'action de la guerre économique. Cette conflictualité n'est plus cantonnée à la sphère politique et aux Etats. Elle a vu apparaitre de nouveaux acteurs issus de la société civile et économique.

Elle a également fait émerger de nouvelles armes où la force n'est plus le maître mot. Dans un monde où l'heure est à la conquête de marché, l'information a une valeur stratégique quelque soit le rapport de force. Aujourd'hui, la société de l'information a modifié la notion de conflictualité. Là où la puissance d'un acteur était mesuré par sa capacité à soumettre l'autre par la force physique, les nouveaux vecteurs induits par cette transformation sociétaire vont être, entre autres, la capacité à maîtriser l'information à la fois produite, protégée et diffusée.

Les rapports de forces traditionnels s'en retrouvent bouleversés par ces tactiques de guérilla ou d'escarmouche informationnelle.

La société de l'information régit notre manière de fonctionner au quotidien. Les acteurs économiques ou étatiques travaillant de plus en plus en réseaux, un nouveau type d'attaque a émergé : les attaques par le contenant. Ces dernières visent à dégrader physiquement les infrastructures de l'autre pour l'affaiblir ou le paralyser. Cependant, à l'ère du web 2.0 et à la démultiplication de la vitesse de circulation des informations, un autre type de d'attaque se dessine : la guerre de l'information par le contenu. Cette guerre compromet l'attaqué par la polémique qu'il est en mesure de créer. Cette attaque a également pour but de dégrader l'image de l'adversaire et de faire réagir, en jouant sur l'émotif, utilisant, entre autre, l'opinion publique comme levier.

La société de l'information a ainsi bouleversé les rapports de force économiques et concurrentiels induisant de nouvelles menaces mais aussi de nouvelles opportunités pour chacun des acteurs.

On peut s'interroger aujourd'hui sur la manière dont on fait la guerre économique par le biais de la société de l'information. En quoi ce nouvel espace de conflictualité a t-il bouleversé les rapports de force économiques traditionnels ? Quelles sont ses caractéristiques et ses armes ?

Partie 1 : La conflictualité par le contenant.

Comme toute guerre, la guerre de l'information commence par des attaques sur les capacités matérielles de l'ennemi. Désormais, toute activité économique repose sur des outils informatiques qui couvrent tous les secteurs, tous les métiers et les relient entre eux. Ces outils souvent connectés appartiennent au cyberespace. Ce dernier, après des années d'insouciance, est devenu un sujet anxiogène car une nouvelle conflictualité est née en son sein. Les attaques informatiques, sur le contenant, ont des modes d'action particuliers qui visent la paralysie ou l'espionnage. Ils ont des conséquences sur le profil des attaquants et sur les réactions des attaqués. Tout cela a créé un nouveau marché et des méthodes de travail qui obnubilent l'approche de la guerre économique.

1.1. La conflictualité dans les systèmes d'information

Les attaques informatiques créent de plus en plus d'inquiétude. Cela est légitime puisque des exemples de plus en plus saillants et nombreux se multiplient. Les attaques les plus connues remontent à une vingtaine d'années. Les premiers virus significatifs datent des années 90 et infestaient les postes individuels de façon aléatoire (*Morris*, *Tchernobyl*, puis *I love you*…)[2]. Par la suite, les attaques se sont étendues aux serveurs qui eux-mêmes infestaient les postes clients. Enfin, depuis les années 2000, des attaques tous azimuts mais ciblées sont apparues. Parmi ces cibles, on distingue les Etats, les institutions et les entreprises.

L'exemple de l'Estonie est le premier d'une longue série. En 2007, le pays balte a en effet été attaqué sur ses systèmes gouvernementaux. La France est également concernée par ces attaques contre des sites institutionnels avec Bercy en 2011[3] qui concernait plus de 10 000 ordinateurs, ou encore celle contre l'Elysée au printemps 2012[4]. On peut aussi citer l'OTAN en 2011[5]. Cette nouvelle conflictualité ne se limite plus aux organismes publics puisque les entreprises elles-mêmes subissent ces attaques. Les entreprises RasGas ou Aramco en ont été

[2] *Les plus grosses attaques informatiques de l'histoire,* Epercut Blog, 19/07/12.
[3] AFP (source), *Le Ministère de l'économie et des finances victime d'une attaque informatique,* Journal Libération, 07/03/11.
[4] J. Guisnel, *Cyberattaques, l'appareil d'Etat visé à deux reprises,* Letelegramme.com,11/07/12.
[5] *http://www.opex360.com/2011/07/22/lotan-cible-dune-troisieme-attaque-informatique-en-un-mois/*

victimes à l'été 2012[6] avec des conséquences toujours croissantes sur lesquelles nous reviendrons. Autre exemple notable, celui du fameux virus Stuxnet[7], initialement dirigé vers les sites de production nucléaire iraniens et qui désormais s'est étendu à des sociétés de par le monde telles que l'américain Chevron[8] ou qui a menacé le français Air Liquide[9].
L'évolution des technologies et la forte croissance de la densité du réseau depuis la fin des années 1990 a de façon évidente été parallèle à celles des cyber-criminels. Le nombre d'utilisateur du réseau internet est passé de 361 millions lors des années 2000 a près de 2 milliards à la fin 2010[10], le réseau des réseaux devenant alors plus dense, technique et offrant par la même une foule croissante d'opportunités. La dernière décennie a vue naitre quatre générations successives d'assaillants aux méthodes et aux buts différents[11].

Le début des années 2000 a principalement été marqué par le défi. Les assaillants utilisent l'attaque par le contenant avec 2 objectifs bien distincts : démontrer leur maitrise de l'outil et leurs capacités de nuisance d'un côté, et de l'autre générer du bruit en soutien à diverses causes. Les conséquences ont été diverses que ce soit pour les entreprises et pour l'utilisateur lambda. En effet, dans cette optique de génération d'écho médiatique, les entreprises et sites les plus populaires ont été les principales victimes de cette génération d'attaquant en recherche de notoriété. Ainsi des entreprises du type de CNN, E-Bay ou bien Yahoo furent les principales cibles, voyant leurs vitrines web rendues complètement inaccessibles. Pour l'utilisateur moyen, ainsi que pour toute entreprise disposant d'un réseau, ce fut l'apparition des premiers virus à forte capacité de nuisance, capables de rendre les machines totalement inutilisables. La propagation a, elle aussi, évolué en ce début de période, passant de la propagation par mail avec téléchargement volontaire (*I love you*, 2000) a l'utilisation de macro-virus, pouvant être inséré au sein d'images ou de document électroniques de type .doc.

La première évolution des profils des ces assaillants a eu lieu aux alentours des années 2004-2005 avec l'apparition d'un objectif clair: rentabiliser cette capacité de nuisance. Ce fut donc l'apparition des *adwares*, petits logiciels installés le plus souvent à l'insu de l'utilisateur, générant l'apparition de publicités ciblées sous forme de *pop ups.* Ce faisant, les entreprises sont clairement devenues clientes de ces services. Les *spyware*, logiciels espions, ont aussi fait leur apparition sur cette période, rendant les pirates possesseurs de quantités

[6] M. Damgé, *Energie : un virus informatique frappe des sociétés du Golfe*, Le Monde.fr, 31/08/12.
[7] *Stuxnet.* Wikipedia.com.
[8] *Le pétrolier Chevron a été infesté par le virus Stuxnet*, Le Monde.fr, novembre 2012.
[9] Valérie Marchive, *Air Liquide assure avoir échappé à Stuxnet*, LEMAGIT, novembre 2012.
[10] *http://www.internetworldstats.com/stats.htm*
[11] *A good decade for cybercrime, Rapport* MC Afee, 2010.

impressionnantes de données sur les utilisateurs du web, données bien évidemment rapidement revendues aux entreprises en exprimant le besoin. Enfin, ce fut l'apparition des premiers réseaux d'ordinateurs zombis, ensemble de machines contrôlées par un seul utilisateur dans le but de réaliser du spamming massif ou de réaliser des attaques de masse à son bon vouloir, et donc de la possibilité de location de ces réseaux pour réaliser des attaques envers ses concurrents.

Suite a l'explosion du potentiel financier un deuxième tournant a eu lieux sur la période 2006-2008 avec les premiers regroupements de criminels sur des modèles semblables, dans leurs organisations et leurs hiérarchies, aux mafias. Ce faisant, ces même assaillants, auparavant en recherche de notoriété sont passés sur des modes d'action bien plus discrets et ont cessé la revendication systématique de leurs actions.

Le dernier tournant en date a été celui du web social, permettant aux individus mal intentionnés de capter des quantités impressionnantes d'informations ciblées sur les utilisateurs à des fins lucratives ainsi que de s'appuyer sur leurs réseau d'amis pour capter des fonds, sur ce qu'il convient d'appeler le *social engineering.* La forte politisation de certains groupes a elle aussi fait son apparition avec l'*hacktivisme*[12].

1.1.1. Types d'attaques et modes d'actions.

L'évolution des attaques présentées *supra* permet d'esquisser une typologie sur les différents types d'attaques et modes d'action. L'analyse de ces points permet de dégager des conclusions sur les postures tactiques prises par les acteurs, c'est-à-dire le choix d'une offensive qui se veut aujourd'hui discrète et indirecte.

Les attaques se différencient en fonction de la couche technique sur laquelle elles s'exécutent. On distingue la couche physique, ou matérielle, de la couche logicielle. Les attaques sur la première couche sont assez rares car elles réclament le plus souvent une action sur le matériel en lui-même alors que le but recherché est d'attaquer à distance. Néanmoins, l'exemple d'Aramco déjà cité a eu pour conséquence l'effacement de disques durs, c'est-à-dire une destruction physique. Il est néanmoins important de remarquer que ce type d'attaque est difficilement réalisable sans l'utilisation d'un agent humain agissant de l'intérieur. Toutefois,

[12] A titre d'exemple, les sites web de *Paypal*, *Mastercard* et *Visa* ont par exemple été rendus inaccessibles par des mouvements de hackers protestataires, utilisant des attaques DDoS, sur de longues périodes, en réaction à la prise de distance effectuée par les 3 entreprises vis-à-vis du réseau *Wikileaks*. L'attaque aura coûté 4,3 millions d'euros à Paypal. Tribunal de Londres, 26/11/2012.

les attaques plus courantes sont logicielles et exploitent les failles des programmes. Le cas le plus courant est le DDoS (Distributed Denial of Service). Parmi ses caractéristiques, on peut citer la facilité de mise en œuvre. Le principe est d'émettre un grand nombre de fausses requêtes en direction d'un serveur afin de le surcharger et le rendre ainsi inopérant. Ce type d'attaque est par exemple celui qui a été utilisé par le groupe *Anonymous* contre le gouvernement ukrainien durant l'été 2012[13]. Typiquement, ce type d'attaque a pour but de bloquer les moyens d'un adversaire. Elles peuvent viser à une élévation de privilèges, c'est-à-dire pouvoir effectuer des actions qui sont généralement impossibles pour l'utilisateur en cours, mais possible par un administrateur. Une personne mal intentionnée peut alors supprimer l'ensemble des données liées à tous les utilisateurs, ou modifier le contenu de fichier afin de servir ses buts.

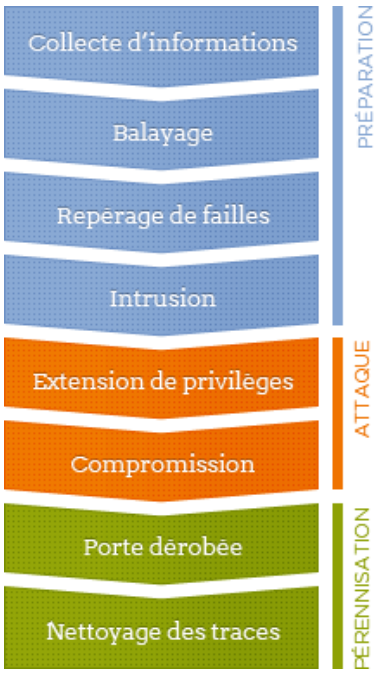
D'autres types d'attaques agissent à la fois sur les couches matérielles et logicielles. C'est le cas des vers (virus qui se répliquent). Une fois implémentés sur un ordinateur, le ver contrôle la machine. Ce contrôle est prévu pour être invisible et permet à l'attaquant une action à distance. La dissémination entraine la mise en place d'un réseau d'ordinateurs zombis qui peuvent eux-mêmes conduire de nouvelles attaques de plus grande envergure. Alors qu'il y a quelques années un seul ordinateur était suffisant pour orchestrer une attaque, désormais un réseau de machine est nécessaire pour la mener à bien. En effet, pour reprendre l'exemple d'une agression de type DDoS, les hébergeurs ont réparti leurs données sur plusieurs serveurs. Cette répartition des moyens complexifie dès lors les attaques. Cette complexification est également observable avec le chiffrement, c'est-à-dire la protection par codes, des accès. Il faut désormais de plus en plus de puissance de calcul pour déchiffrer les codes ou les trouver.

Ces exemples permettent de montrer que les attaques sont avant tout discrètes : il n'y a pas de préavis dans la guerre informatique. La discrétion qui accompagne ces actions ajoute un degré de dangerosité pour les entreprises, qui n'identifient pas toujours les attaques dont elles sont victimes car elles sont indirectes. En effet, les attaquants sont difficiles à identifier car ils ne revendiquent pas généralement leurs actions.

[13] Emil Protalinsky, *Anonymous attacks Ukrainian government after demonoid bust*, in Zdnet.com, août 2012.

1.1.2. Rythmes et phases.

Dissimulées, les actions ont des rythmes particuliers dans les attaques du contenant qui peuvent être à la fois fulgurantes, lentes ou cycliques. La vitesse est une des caractéristiques des systèmes d'information. Les attaques sur ces moyens peuvent s'effectuer avec une grande rapidité. Le cas des DDoS est un exemple de rapidité puisque sans avertissement, une entreprise peut voir ses systèmes débordés en quelques instants. Une attaque peut se décomposer en phases d'observation, d'infiltration, d'attaque en force puis de gestion des effets produits. Ce cycle tactique est classique et rappelle les principes militaires : acquisition et exploitation du renseignement, conception, préparation, réalisation, exploitation. C'est ainsi le cas de Stuxnet dont la préparation semblerait avoir débuté en 2006 et aurait suivi la construction suivante :



Source : http://www.kommunauty.fr/article-825-stuxnet-on-reprend-tout-a-zero

La question du rythme et de la répétition se pose également. Néanmoins, elle est mal-à-propos. Toute attaque entraine en effet une adaptation du défenseur. Dès lors, immunisé, ce dernier est paré. La relation entre l'attaquant et l'attaqué apparait dès lors comme primordiale dans l'étude de cette conflictualité puisqu'elle est évolutive.

1.1.3. Rapports de force et timing.

La question du rapport de force et du moment de l'attaque est importante pour les attaques par le contenant. Les exemples déjà cités montrent des rapports de forces très divers. Il n'est pas possible de conclure que ce type de conflit donne l'avantage au faible ou au fort. En effet, les pirates sont fréquemment assimilés à des faibles s'attaquant à un fort comme une entreprise. Toutefois, autant ce principe est admissible pour une attaque menée par un pirate isolé, autant les organisations nouvelles telles qu'*Anonymous* ou les mafias internationales qui sont constituées de nombreux de pirates. Dès lors, ceux-ci peuvent difficilement être assimilés à des faibles. De plus, l'exemple de Stuxnet très certainement piloté par un ou plusieurs Etats montre lui aussi que l'attaquant peut être un fort. A l'inverse, un attaqué peut être un faible dans le cas d'une attaque d'un individu ou d'une entreprise modeste. Toutefois, un grand groupe avec ses propres moyens informatiques, ses personnels spécialisés, ses procédures et moyens de protection est un fort. Par conséquent le rapport de force ne parait pas pertinent pour analyser la typologie du rapport de force dans la guerre par le contenant.

En revanche, si la clef de la décision ne réside pas dans une asymétrie des forces des acteurs, elle semble être liée au moment de l'action. Le *timing* est clef. Comme souvent dans les mouvements tactiques, la surprise est un élément fondamental. C'est le cas dans les attaques informatiques. Il n'existe pas dans ce type de conflit de stratégie, de règles, de lois de la guerre. La menace n'est pas directive et temporelle. Elle est multidirectionnelle et permanente. L'attaque est toujours lancée avec surprise afin de tenter de décupler les effets produits. C'est donc plutôt le temps de l'action, le *timing*, qui semble plus pertinent que le rapport de force.

1.2.Conséquences économiques et organisationnelles.

L'augmentation de la dangerosité sur les réseaux et la diversification des modes d'attaques a poussé les entreprises à se défendre. Cela a permis au marché de la sécurité informatique de se développer considérablement sur la dernière décennie, et ce à juste titre, dans la mesure où, en 2006, 90% des entreprises américaines reconnaissaient avoir rencontré un problème de sécurité informatique sur les 12 derniers mois pour un montant total de 194 millions de dollars US de perte[14]. Bien que le marché de la sécurité informatique soit florissant[15], il est à noter qu'aucune protection totale n'existe dans la mesure ou les 3 principaux type d'attaques

[14] R. Richardson,12th annual computer crime and security survey., Computer security institute, 2006
[15] Internet Crime report, NWCCC et FBI, 2006.

rencontrés par les entreprises sont les suivants[16]: la fraude financière, qui se fonde le plus souvent sur le manque de formation ou de connaissance du personnel, trop enclin à fournir de l'information, puis les virus, vers et chevaux de Troie, transitant à hauteur de 74% par e-mail et enfin la pénétration des systèmes par des agents extérieurs avec pour objectif le vol de donnée ou l'altération du bon fonctionnement du système. Donc, sur trois des principaux vecteurs d'insécurité pour les entreprises, deux sont en grande partie fondés sur le personnel même de l'entreprise. Le *Computer Security Institute* estime que 64% des pertes financières des entreprises dues à des problèmes de sécurité informatique sont de la responsabilité, volontaire ou non, des employés et rappelle que près des trois quarts des entreprises dépensent moins de 5% de leurs budgets IT[17] sur la formation et la prévention informatique aux Etats-Unis.

1.3. Nouveaux marchés.

Les menaces qui pèsent sur les systèmes d'information ont engendré l'émergence de nouveaux marchés. Le premier concerne la protection. Dès les premières attaques des années 90, le réflexe des entreprises a été de se doter de logiciels ou matériels pour se protéger. Parmi ceux-ci, on note principalement les antivirus, antispywares, firewalls… Désormais, les produits disponibles prennent en compte l'ensemble des menaces et assurent la protection des couches matérielles et logicielles. Sur ce marché, des entreprises très hétérogènes en termes de taille se sont positionnées. Ainsi, les plus connues sont *Norton*, *McAffee*, *Trend*, *Symantec*, *Avast* ou même *Microsoft*. Néanmoins, des entreprises plus modestes existent sur le marché : *Arkoon*, *Panda*, *AVG*… Les fabricants de matériels sont également présents, à l'image d'*IBM* ou d'*Intel*. Ce marché est extrêmement florissant et actif. Il a ainsi crû de 7,5% en 2011 avec un chiffre d'affaire de 17,7 milliards de dollars cette même année[18], et ceci en pleine crise.

[16] 60 milliards de dollars pour l'année 2012 selon l'estimation du cabinet américain Gartner, soit 8,4% de hausse par rapport à l'année précédente.
[17] Information Technology
[18] http://www.gartner.com/

Tableau : Chiffres d'affaire et parts de marché des entreprises de sécurité informatique

Entreprise	**CA 2011**	**Parts de marché 2011 (%)**	**CA 2010**	**Evolutions 2010-2011 (%)**
Symantec	3,652.0	20.6	3,121.6	17.0
McAfee	1,226.0	6.9	1,691.6	-27.5
Trend Micro	1,205.1	6.8	1,082.5	11.3
IBM	930.1	5.3	814.7	14.2
EMC	716.1	4.0	626.6	14.3
Others	9,985.8	56.4	9,137.2	9.3
Total	**17,715.1**	**100.0**	**16,474.2**	**7.5**
Source: Gartner (April 2012)				

Le second marché engendré par l'émergence des menaces sur les systèmes d'information concerne les attaques. Il demeure, certes, des acteurs qui agissent de façon financièrement désintéressée. Toutefois, certains sont rémunérés. Ils le sont pour développer la protection comme *Microsoft* qui a recruté en 2011 un jeune pirate informatique de 11 ans[19]. Cette nouvelle forme de travail a son marché. C'est le cas dans les actions d'espionnage puisque les acteurs cherchent à vendre les données dérobées. C'est le cas sur des forums ou sites tels que *Shadowcrew* qui agit de 2002 à 2004 dans la revente de numéros de cartes de crédits[20]. Ces forums ou sites sont évidemment clandestins. D'autres acteurs agissent dans les actions de destruction. Les informations les concernant sont évidemment difficiles à obtenir. Pour certains, ils seraient une centaine dans le monde capables de lancer de véritables attaques sur demande[21]. Dans ce cas, ils sont souvent mandatés par des entreprises concurrentes comme les sites Distant-Replays et Jersey-Joey qui ont été attaqués en 2005 par un jeune hacker indien de dix-sept ans[22]. D'autres cas ont émaillé la presse dans le cadre de l'espionnage ou de la surveillance. C'est le cas avec *EDF* qui a été condamné en novembre 2011 pour avoir mandaté des pirates afin d'espionner *Greenpeace*[23].

[19]*Un pirate de 14 ans engagé par Microsoft*, in Ecommerce-infos.com, mai 2011.
[20] Shadowcrew, Wikipedia.com
[21] Charles Haquet, *Qui sont les mercenaires de la cyberguerre*, L'express, 23/11/12.
[22] http://www.zataz.com/news/17802/ddos--coulisse--attaque--informatique.html
[23]Hanna Guersmann, *EDF fined EDF fined €1.5m for spying on Greenpeace*, The Guardian, 10/11/11.

Bien que les marchés de la sécurité/attaque soient devenus florissants suite à l'explosion de ces pratiques illégales, le constat est moins glorieux sur le volet légal. En effet, les attaquants, et très souvent les entreprises clientes de leurs services, ne sont pas poursuivis. Selon *Cybercrimeswatch,* 25% des crimes informatiques ne sont pas résolus et ce pour diverses raisons outre la forte habilité des assaillants à agir discrètement et de manière à ne pas laisser de possibilité de remonter jusqu'à eux[24]. Les principales raisons de cette relative impunité résident dans l'aspect transnational de ces acteurs et dans les disparités législatives existantes entre les Etats dans le domaine informatique. Même si les Etats-Unis, la Chine et l'Allemagne représentent à eux seuls près du tiers des crimes[25], le phénomène est désormais mondial et ne peut être que difficilement contré par les appareils législatifs étatiques sans une réelle volonté commune. Mais cette volonté n'est clairement pas établie, surtout de la part de certains Etats, comme la Chine. Cette dernière n'a arrêté que 460 hackers dans le courant de l'année 2010[26] et les agissements des cybercriminels chinois à l'encontre des entreprises étrangères, américaines le plus souvent, ne semblent pas déranger outre mesure le pouvoir en place[27].

1.4. Eléments de conclusion sur la guerre économique par le contenant.

L'étude du champ d'action de la guerre par le contenant nous amène à réaliser plusieurs remarques.

Tout d'abord, ces attaques sont de plus en plus nombreuses, vastes et surtout efficaces comme l'a montré l'exemple d'Aramco à l'été 2012. Les réactions sont nombreuses et accaparent toutes les entreprises utilisant des moyens informatiques, notamment pour mettre en place des politiques de protection. Outre le volet protection, celui de la prévention est tout aussi important pour les entreprises. Il est très difficile de quantifier de façon précise les coûts induits, toutefois ceux-ci sont extrêmement importants, surtout pour réparer les préjudices. Les estimations précédemment citées évoquaient des sommes supérieures à 270 milliards d'euros en 2010[28], même s'il faut tempérer ces chiffres en soulignant qu'ils sont produits par les fournisseurs de sécurité informatique.

De plus, ces attaques se montrent finalement limitées, car concentrées dans l'espace et le temps. En outre, ces conflits informatiques restent illégaux, le terme de piraterie est donc justement choisi. Les procès tendent à se multiplier car les législations nationales et

[24] http://www.cybercrimeswatch.com/cyber-crime/cyber-crime-statistics.html
[25] Symantec, 2012 Norton Cybercrime report, 2012.
[26] *Plus de 460 hackers chinois arrêtés cette année*, Le Monde, édition du 01/12/2010.
[27] *WikiLeaks : Pékin aurait commandité le piratage de Google*, Le Monde, édition du 29/11/2010.
[28] Mathieu Neu, *IT-Piratage informatique : les PME, trop insouciantes pas assez paranoïaques*, 09/02/12.

internationales commencent à s'adapter pour protéger leurs économies. D'ailleurs, les études, doctrines et les créations d'instances spécialisées montrent l'intérêt que portent les Etats pour ces faits. Déjà en 2008, le *Livre blanc sur la défense et sécurité nationale* évoquait en France ces questions. Plus encore, les premiers éléments sur sa prochaine édition en 2013 laissent entendre que la cyberdéfense restera une priorité nationale[29]. Or, ce concept de cyberdéfense est important à ce stade de la réflexion car il accapare toutes les attentions.

En effet, la guerre de l'information est exagérément vue comme étant consubstantielle à l'existence du cyberespace. Ce dernier est un terme répandu dont le préfixe est excessivement employé : cyber-menaces, cyber-terrorisme… Puisque cette guerre de l'information se déroule sur les réseaux mêmes, il convient de définir ce qu'est le cyberespace. Cela n'est pas aisé puisque deux approches semblent s'affronter : une plus technique, l'autre plus humaine. Le premier type de définition est celui adopté par l'ANSSI[30] en France. Cette dernière voit dans le cyberespace : *« l'espace de communication constitué par l'interconnexion mondiale d'équipements de traitement automatisé de données numérisée[31] »*. Une autre vision voit plutôt le cyberespace comme étant : « l'espace constitué des systèmes d'information de toute sorte connectés en réseaux et permettant la communication technique et sociale d'informations par des utilisateurs individuels ou collectifs[32] ». Cette deuxième définition correspond mieux à notre avis à ce qu'est le cyberespace. En effet, elle ajoute un élément fondamental : l'information. En somme, la technique n'est là que pour permettre de l'échange d'information par une action humaine. C'est pourquoi la guerre économique ne s'effectue pas uniquement sur les matériels et les logiciels, mais par le biais également de l'information elle-même. Cette guerre de l'information est celle du contenu.

[29] *La France fera de la Cyberdéfense une priorité nationale*, Numerama.com, 30/11/12.
[30] Agence Nationale de la Sécurité des Systèmes d'Information
[31] ANSSI, *Stratégie de la France. Défense et sécurité des systèmes d'information*, Paris, février 2011, p.21
[32] Kempf Olivier, *Introduction à la cyberstratégie*, Economica, 2012, p.14

Partie 2 : La guerre de l'information par le contenu.

2.1. La société de l'information : un relais d'opinion aisément accessible pour faire la guerre économique

La société de l'information s'est imposée au fil des années comme un nouveau champ d'affrontement économique et concurrentiel. Elle a profondément modifié la nature des affrontements. Là où l'on mettait auparavant des mois à rechercher la faille de son adversaire et le scandale potentiel pour ensuite le communiquer, la société de l'information permet aujourd'hui de diffuser un message rapidement, quel qu'il soit, en le rendant accessible à tous sans avoir besoin de diligenter une campagne de communication construite et coûteuse. Par le biais des outils de diffusion qui la composent (réseaux sociaux, internet, médias…), elle permet la diffusion rapide de messages auprès d'un public large ce qui lui octroie une puissance à la fois temporelle et géographique sans égal auparavant. Contrairement aux champs économiques traditionnels, elle rend possible l'intervention d'acteurs de la société civile[33] qui l'utilisent comme un relais d'opinion et un moyen d'affrontement privilégié, tel l'ONG lançant par les médias ou internet une campagne d'opinion contre une entreprise ou un Etat.

L'attaque informationnelle par le message[34], appelée guerre par le contenu[35], a donc pris avec l'avènement de la société de l'information une puissance importante face à laquelle chaque individu, organisation et entreprise doit aujourd'hui se prémunir.

L'espace conflictuel de la société de l'information a pour caractéristique d'être ouvert. Ses vecteurs, notamment Internet, suppriment la notion de frontière[36] (temporelle et géographique). L'information est ainsi disponible tout le temps, de manière instantanée entre le moment où l'on dépose son message et le moment où il est à la disposition de tous. Il a donc pour caractéristique de modifier l'échiquier d'affrontement, qui lui octroie une audience sans égal. Ces éléments procurent au message diffusé un effet multiplicateur et donc une résonnance importante. Il faut néanmoins noter que cette résonnance est réelle si le message touche sa cible.

---

[33] Harbulot, D. Lucas, *La guerre économique à l'ère de la société de l'information*, AEGE, 2008.
[34] Ce qui la diffère de l'attaque informationnelle par le bais d'une technologie (cf partie 1).
[35] La guerre de l'information par le contenu correspond à l'ensemble des pratiques offensives destinées à déstabiliser un adversaire par le biais d'un message polémique ou par le dénigrement. (in C. Harbulot, D. Lucas, *La guerre économique à l'ère de la société de l'information*, AEGE, 2008.)
[36] C. Harbulot, *La main invisible des puissances*, Ellipses, 2007, Paris.

2.2. La guerre de l'information : une guerre de représentations

Les médias comme internet sont devenus des terrains actifs d'attaque et de défense. Ces attaques informationnelles[37] utilisent notamment la polémique. Cette dernière repose, entre autre sur la critique de pratiques menées par des entreprises ou des dirigeants, la qualité ou les dangers d'un produit… Ces manœuvres peuvent être fatales pour l'image des entreprises.

La réussite d'une attaque informationnelle repose sur le message constitué. Il s'agit de définir un message qui aura la plus grande résonnance informationnelle. Cette dernière passe souvent par la recherche de la faille[38] de son adversaire, celle qui aura le plus de résonnance auprès des acteurs que l'on souhaite rattacher à sa cause. L'objectif est de toucher les sensibilités et les représentations de l'opinion (par le biais de photos, vidéos…) via la mise en exergue de questions éthiques. Les auteurs d'attaques informationnelles n'hésitent pas à créer des preuves, avoir recours au mensonge afin que leur message soit le plus crédible, audible et visible. Ce type de pratiques s'apparente à la désinformation.

Les attaques informationnelles dans le domaine sanitaire sont particulièrement caractéristiques. On cherche à dénigrer un produit en expliquant à l'opinion sa dangerosité sur la santé humaine. L'affaire du saumon d'élevage[39] est un très bon exemple de manipulation informationnelle dans un but de déstabilisation concurrentielle. Une revue américaine scientifique a publié en 2004 une étude sur les polluants présents dans le saumon d'élevage et sauvage soumis à la consommation. Cette étude pointait du doigt la dangerosité du saumon d'élevage. Elle fut très rapidement reprise dans les médias américains avant de rebondir en Europe. Au moment de la diffusion de l'étude, le saumon sauvage du Pacifique était en perte de marché face au saumon d'élevage européen (Ecosse et Norvège).

« L'affaire du saumon », comme elle fut nommée par la suite, a fait grand bruit dans le monde occidental et impacté dans un premier temps les ventes de saumon d'élevage. Il a été révélé plus tard que cette étude avait été financée par une fondation américaine (Pew Charitable Trusts) dont le Président avait des parts dans une pêcherie en Alaska.

[37] C. Harbulot, *La main invisible des puissances*, Ellipses, 2007, Paris.
[38] Thématiques qui vont heurter la sensibilité ou retenir l'attention de l'opinion cible.
[39] *Le Saumon*, Document de présentation, Eurodecision-AIS, 14 mais 2004.

L'affaire du saumon est un très bon exemple de campagne de désinformation en contexte de guerre concurrentielle. Ses auteurs ont usé de la caution scientifique pour attirer l'attention des médias afin que leur message soit relayé vers le plus grand monde.

Les campagnes de désinformation sur les sujets éthiques sont également nombreuses. La société française SODEXO en a été victime aux USA entre 1999 et 2002. Sur cette période, elle a été l'objet d'attaques diligentées par le syndicat américain SEIU centrée sur l'organisation et son mode de travail. La société a été accusée de discrimination raciale, mauvaises gestion RH … L'objectif des attaquants était de toucher l'image et la culture de l'entreprise[40].

Les attaques informationnelles ne mobilisent pas seulement les acteurs de la société civile. Elles peuvent également être instrumentalisées par des Etats comme cela a pu se passer en Bolivie et Argentine à la défaveur de Suez[41].

2.3. Les vecteurs induits par la société de l'information.

Les vecteurs utilisés pour diffuser les messages ont une importance toute particulière dans la stratégie informationnelle. A chaque vecteur correspond une temporalité et des cibles. Le message seul n'est pas suffisant, la bonne gestion du vecteur est une nécessité pour la réussite de sa campagne informationnelle.

La gestion du temps dans le cadre de l'attaqué.

L'attaque se fait en général rapidement avec un degré de déstabilisation fort. Cela enferme de fait l'attaqué dans une rhétorique justificative dont il est très difficile de se sortir. Cette justification donne de plus en plus de crédit à l'attaquant en faisant perdre la face à l'attaqué. Il n'existe pas de règle d'or sur le timing de l'attaque, on notera malgré tout que certaines règles sont observables[42]

[40] C. Harbulot (dir), *Manuel de l'Intelligence économique*, collection Major, PUF, Paris, 2012, p239.

[41] En 2004-2005, Suez a été victime d'une grande campagne d'information qui l'a conduit de temps plus tard à quitter ces deux pays dans lesquelles elle avait un monopole d'exploitation dans le domaine de la gestion et de la distribution de l'eau potable. Au début des années 90, la société Suez est accueillie à bras ouvert par les gouvernements argentins et boliviens pour remettre d'aplomb les systèmes de gestions de l'eau. L'entreprise réalise ainsi de gros investissements. Quelques années plus tard, elle demande aux gouvernements d'augmenter ses tarifs. A ce moment là, les pays subissent quelques difficultés économiques et la population n'est pas prête à voir le prix de l'eau potable augmenté.
L'information selon laquelle Suez souhaite augmenter les prix de l'eau filtre rapidement dans la société civile. L'entreprise se retrouve donc la cible de manifestations de rue, grèves, campagnes médiatiques…). Face à la pression populaire, les gouvernements enjoignent la société à quitter le pays. Suez perd ainsi deux gros marchés en Amérique du Sud et voit son image fortement écornée.

[42] L. Gaildraud, C. Harbulot, *Orchestrer la rumeur, Rival, concurrent, ennemi… comment s'en débarrasser !*, Eyrolles, Paris, 2012.

Pour l'attaqué, la gestion du temps est primordiale dans le sens où il arrive dans une gestion de crise. Dans les cas de déstabilisation d'entreprises lancée par des ONG, la réponse doit être, en générale, rapide et brève. Sans entrer dans la justification ou dans le déni, il est nécessaire de communiquer sur une crise pour rassurer à la fois ses clients et fournisseurs.

- **Les différents types de vecteurs**.

- Mass médias (journaux numériques, TV et papier)

L'impact du message est fort. Médias qui bénéficient d'une grande crédibilité auprès de l'opinion publique (i.e. : mention « vu à la TV). La diffusion se compte en heure avec les éditions numériques ou les chaînes d'information continue. Un argumentaire est beaucoup plus facile à faire sur tout type de sujet car il y a possibilité d'expliquer par l'image et la parole.

- Réseaux sociaux de masse (Facebook et Twitter)

Message qui se doit d'être concis, vendeur et travaillé pour l'impact et publié initialement par une entité ayant une certaine légitimité. Formidable outils de communication, une information peut faire le tour du monde en quelques secondes. Le message sera rapidement repris pour être traduit dans toutes les langues faisant tomber les frontières. Phénomène de masse et facilité de compréhension du message sont les clés de la diffusion mondiale sur ces réseaux.

*2.*4. Quelles atteintes ? Quelles forces ?

Les atteintes sont aussi diverses que leur force sur le public et la cible visés. Tout est lié à la force du message et sa réceptivité.

Les attaques par le contenu sont souvent basées sur les mêmes sujets ("*la qualité des produits, la sécurité sanitaire, le comportement des dirigeants, la santé financière d'une société, l'opacité des comptes, les pratiques de concurrence déloyale, le non-respect des règles d'environnement »*[43]…). Elles affectent l'image de l'entreprise et poursuivent des buts précis utilisant une caisse de résonnance permise par le développement de la société de l'information :

[43] C. Harbulot, *La main invisible des puissances*, Ellipses, 2007, Paris.

- Image

L'image ne rapporte pas directement un retour sur investissement à l'entreprise d'où le fait qu'elle ne soit pas protégée en priorité à quelques exceptions près. La guerre de l'information par le contenu va sa focaliser sur un aspect qui ne rentre pas dans le bilan de l'entreprise : sa réputation.

Cet aspect ne rentrant pas dans le patrimoine de l'entreprise et n'ayant pas de Retour Sur Investissement directement mesurable, il n'est pas considéré comme stratégique, les dirigeants préférant assumer la gestion de crise, souvent beaucoup plus coûteuse que l'anticipation des risques

Les conséquences de l'affaiblissement de l'image de l'entreprise peuvent être multiples, et sont motivées par le fait que l'attaquant va pouvoir agir suite au déchaînement médiatique. Ci-dessous, les conséquences les plus observées lors d'une attaque par le contenu

- Préparer une OPA **:**

Une chute du cours de l'action qui peut favoriser une OPA. L'exemple de Danone [44]qui a racheté la branche biscuit de Lu pour la moderniser est très parlant. A ce moment Danone a été déstabilisé par une attaque informationnelle concernant un vaste plan de licenciement[45]. Danone a dû, pour faire face à ces pertes, vendre la branche biscuit de lu à un prix dérisoire. Dans ce cas, il est très difficile d'identifier le commanditaire de l'action.

- Interdire l'accès à un marché d'une entreprise

Par une attaque sur l'image d'une entreprise, l'attaquant peut pousser une nouvelle norme interdisant simplement l'accès au marché à une entreprise. L'exemple de l'interdiction pour la SNCF de se positionner sur le marché américain en raison de son rôle dans la déportation des juifs pendant la guerre[46].

[44] Cours de Guerre ou Intelligence économique, 2010, Loïc LUCAS et Odile BOIZARD, Euromed Management
[45] http://www.communication-sensible.com/download/analyse-crise-lu-danone-2007.pdf
[46] DOMART Quentin, *« SNCF, la bataille du rail américain »*, Business International, page 74-77, 1janvier 2011

- Affecter la gouvernance de l'entreprise

L'affectation de la gouvernance d'une entreprise peut se traduire par le débauchage de salarié mais aussi par un limogeage qui nuira à l'avancement de la stratégie de l'entreprise sans compter les dommages collatéraux concernant l'entreprise. Renault a été victime de ce genre d'attaque lors de l'affaire de la livraison des plans de voitures électriques en Chine[47].

2.5. Le renversement des rapports de force traditionnels : l'attaque offensive l'emporte sur les adversaires en posture défensive.

L'affrontement économique et concurrentiel dans la sphère informationnelle modifie les rapports de force traditionnels. La notion d'acteur fort ou faible se trouve complètement bouleversée. La puissance d'un Etat, d'une ONG ou d'une entreprise n'est plus un facteur pour le définir en tant que fort ou faible. L'avantage est donné généralement à l'acteur offensif quelle que soit son origine.

Le fort devient celui qui a l'avantage informationnel poussant l'attaqué à se justifier. La posture justificative met l'attaqué dans une situation défensive. La conséquence de l'attaque étant l'enfermement de l'adversaire dans cette position. Une telle position réduit la marge de manœuvre de l'attaqué l'enfermant dans un discours justificatif. Ce discours justificatif chez l'attaqué empêche toute réflexion sur la contre-attaque et le pousse à la faute.

C'est la gestion de l'information dans le temps et donc l'anticipation qui crée la force. La force n'est pas liée à la notoriété de l'acteur mais à sa capacité à manœuvrer l'information.

Au printemps 2010, Nestlé a été victime d'une attaque informationnelle menée par Greenpeace sur l'usage de l'huile de Palme[48] dans ses produits. L'attaque est partie d'une vidéo diffusée sur internet associant les produits de Nestlé à des animaux. Nestlé n'a pas au départ considéré le potentiel de cette attaque et s'est contenté de condamner en justice pour faire retirer les vidéos. Cette condamnation a permis à Greenpeace de rebondir et d'alimenter le buzz sur son mouvement. La crise informationnelle s'est cristallisée sur la page Facebook de Nestlé dont la gestion a été très mal orchestrée par le Community Manager, ce qui a beaucoup entaché l'image de l'entreprise.

La direction de Nestlé a mis beaucoup de temps pour prendre en considération les dangers de cette attaque. Il lui a fallut des échecs successifs et l'exportation de la campagne

[47] *Le déroulement de l'affaire Renault*, L'Usine Nouvelle, 2011.

[48] L'exploitation de l'huile de palme dans les forêts indonésiennes est accusée d'être responsable de la déforestation du pays et la disparition de certaines espèces endémiques.

informationnelle vers les principaux médias de grande écoute français pour qu'elle adopte une stratégie réactionnelle qui n'était finalement pas adoptée à la situation.
De manière générale les attaques informationnelles sont peu anticipées par les entreprises. Elles se contentent à tort de gérer la crise plutôt que de l'anticiper prenant le risque de voir leur entité fortement impactée. Les conséquences peuvent cependant parfois être importantes, surtout quand l'attaque par le contenu est liée à celle par le contenant.

Partie 3 : L'association de l'attaque par le contenant et le contenu : le nouvel art de la guerre.

Les attaques du contenant et du contenu ont des portées de plus en plus majeures pour les entreprises. Même si des différences fondamentales existent entre les deux sur le fond contenant et contenu ont des caractéristiques communes. Ces caractéristiques peuvent être combinées, ce qui produit des effets redoutables car ils sont notamment multidirectionnels. Or, ce nouvel art de la guerre est trop souvent sous-estimé même si son intérêt commence à se développer notamment au travers du développement de l'*e-reputation* et du *personal-branding*.

3.1. Attaques par le contenant, attaques par le contenu : des différences fondamentales sur le fond.

La comparaison des deux types de conflits permet de distinguer des similitudes et des différences quant aux acteurs, modes d'action, cibles, effets et lisibilité lorsqu'ils sont mis en œuvre.

On distingue généralement trois catégories d'acteurs dans le cyberespace[49] :

- *Les acteurs individuels*

  Internaute, consommateur, travailleur, opineur, citoyen, fraudeur, le veilleur colporteur, l'identifié

- *Les acteurs collectifs*

  Entreprises, notamment celles des technologies de l'information, médias, partis politiques, groupes idéologiques, églises, syndicats, écoles, associations, mafias, groupes criminels, pirates, terroristes, hacktivistes, groupes de circonstance

[49] Olivier Kempf, *Introduction à la cyberstratégie*, Broché, Paris, 2012.

- *Les acteurs étatiques*

  Gouvernements, administrations, collectivités territoriales, police, armée, services, organisations internationales.

A la lecture de cette catégorisation, il apparait que certains acteurs peuvent agir indistinctement dans le contenant ou dans le contenu. Les cas les plus emblématiques sont les Etats pour lesquels il est avéré qu'ils utilisent ces deux types d'attaques. Encore une fois, l'exemple des Etats-Unis apparait symptomatique avec *Stuxnet* pour le contenant et leurs Gongo[50] pour le contenu. Cette capacité à jouer sur les deux tableaux est évidemment possible pour d'autres acteurs économiques même si les exemples sont plus confidentiels.
En somme les acteurs du cyberespace agissant sur le contenu ou le contenant peuvent être les mêmes. Cette association leur donne des effets plus accrus.

Les deux types d'attaques se distinguent sur les cadres dans lesquels elles interviennent et sur les modes d'action utilisés. En effet, l'attaque par le contenant se focalise sur les moyens matériels et a pour but de paralyser ou de voler. Les modes d'action sont le plus souvent des attaques en force (DDoS), c'est-à-dire directes. Néanmoins, pour certains besoins l'attaque peut être indirecte afin de contaminer les outils informatiques même si ces contournements restent limités en nombre. Les cibles restent toujours identifiées et identifiables par les effets produits, même si les dommages collatéraux restent possibles. Pire, une attaque par le contenant peut être réversible, se retourner contre son auteur. Cet « effet boomerang » est un risque important que le virus Stuxnet[51] illustre une fois de plus. Les effets les plus importants sont finalement ceux de la récupération d'information stratégique. Concernant la visibilité, ces attaques sont furtives et recherchent la discrétion. Elles sont connues et identifiables généralement après.
Les attaques par le contenu sont, elles, différentes. Elles ont évidemment un objectif et donc une cible. Néanmoins elles sont indirectes puisqu'il leur est nécessaire d'utiliser des caisses de résonance afin d'amplifier leur force. Cette diversion est avant tout une quête de force extérieure alimentée par différents canaux. Le but est souvent plus ambitieux que les attaques par le contenant car les effets sont plus notables : la destruction ou l'affaiblissement sont recherchés.

[50] *Government organized non-governmental organization*
[51] Voir partie 1.

La comparaison des effets produits par ces types d'attaques montre que l'attaque par le contenu a des effets potentiellement plus importants que l'attaque par le contenant. L'idée de les associer parait alors intéressante et potentiellement redoutable dans le cadre de la guerre économique.

3.2. Contenant/contenu : une arme redoutable en combiné

Les attaques associant des tentatives de destructions matérielles et immatérielles à destination d'acteurs économiques et étatiques se sont multipliées ces dernières années. Elles visent à la fois le piratage des moyens techniques de la cible et son image.
Cette combinaison de moyens et de modes d'actions est particulièrement difficile à détecter en amont, ce qui en fait une arme particulièrement redoutable.
Un grand groupe français[52] a été victime d'une attaque de ce type. Les attaquants ont lié les adresses mails professionnelles de certains dirigeants de l'entreprise à un site pédophile avant de les dénoncer à la police locale. L'affaire a très rapidement été reprise dans les médias et poussé l'entreprise à licencier les dirigeants incriminés malgré leur innocence. L'attaque décrite ici a atteint à la fois des moyens techniques de l'entreprise (boites mail piratées) et son image (association du groupe à des actes pédophiles).

A la lumière de cet exemple, on observe qu'une attaque par le contenant peut être lancée afin de préparer le terrain pour le contenu. En effet, comme il l'a été expliqué précédemment, certaines attaques par le contenant permettent soit à une élévation des privilèges, soit d'accéder à des bases de données. Dans le second cas, ce sont les bases de mots de passes qui sont visées. Ces dernières ont permis aux hackers d'usurper l'identité des utilisateurs sur le système visé, ce qui leur a permis alors d'effectuer l'attaque par le contenu. Ainsi, le message délivré est plus impactant suite à une modification du système de l'entreprise. Le système sert à créer et héberger la preuve de l'attaque informationnelle.

[52] C. Harbulot, D. Lucas, *La guerre économique à l'ère de la société de l'information*, BDC AEGE, 2008, p5.

L'association des attaques par le contenant et le contenu est une nouvelle arme de guerre informationnelle particulièrement redoutable. Elle reprend les fondamentaux de l'art de la guerre, faire du bruit à l'ouest pour attaquer à l'est[53]. Dans le cadre d'une action combinée, contenant-contenu, l'un est souvent le leurre d'un autre.

3.3. La menace par le contenant et le contenu sont appréciées de manières différentes par les acteurs économiques.

Nous pouvons aujourd'hui réaliser un constat. L'attaque par le contenant et celle par le contenu, au delà de leurs différences structurelles, ne sont pas appréhendées de la même manière par les acteurs qui en sont victimes alors que toutes deux sont des armes particulièrement acérées dans un contexte de guerre économique.

L'attaque par le contenant reste aujourd'hui le type d'attaque le plus connu et appréhendé. Nous avons tous en tête l'image du hacker et du virus qui atteint le serveur informatique ou votre ordinateur. Cette menace est d'autant plus perceptible pour nous tous qu'elle nous menace tous directement[54]. Les recours à un anti-virus ou à de multiples des pare-feux sont donc monnaie courante. Pour un acteur économique, il est donc aisé de justifier de consacrer des budgets à sa destination.

Pour sa part, l'attaque par le contenu est plus complexe à appréhender et à prévenir. En effet, nous sommes tous abreuvés chaque jour d'informations, de scandales multiples. En tant que « public », « lecteur » des médias ou d'internet nous avons globalement des difficultés à détecter les attaques informationnelles. Cette difficulté en fait d'ailleurs toute sa force. Le grand public comme les acteurs économiques ont donc peu conscience de la dangerosité des messages dont ils sont destinataires. Peu conscients des dangers, ils ne pensent pas à s'en protéger.

L'attaque par le contenant et celle par le contenu opposent deux processus d'atteinte. L'une est matérielle et mesurable aisément : celle par le contenant. L'autre est beaucoup plus complexe et immatérielle : celle par le contenu.

Cette opposition explique la différence d'investissement et de préparation des entreprises à l'égard des attaques informationnelles.

[53] Les 36 stratagèmes.

[54] La crainte de voir son ordinateur touché par un virus ou son compte internet (site, réseaux sociaux…) piraté est présente dans les esprits de tous les utilisateurs.

3.4. L'émergence de la e-reputation et du personnal branding.

Avec l'avènement de la société de l'information et notamment des outils internet, les acteurs économiques ont progressivement compris qu'il fallait qu'ils soient présents sur internet. On retrouve désormais en nombre les entreprises ou personnalités qui possèdent leur page Facebook ou leur compte Twitter sur lesquels ils délivrent chaque jour des nouvelles de leur marque. Cette présence est nouvelle et résulte d'une prise de conscience progressive qui pourrait être rapprochée des retours d'expérience récents en matière d'attaque informationnelle. On parle désormais d'e-réputation pour qualifier l'image d'une entreprise sur leweb. La e-reputation est un concept qui a pris de l'ampleur à partir de la fin de l'année 2008[55]. Il existe de nombreuses définitions[56] de ce terme. Il peut être résumé de la manière suivante : il s'agit de l'image que les internautes ont d'une entreprise en fonction de ce qu'elle est sur Internet. Ce concept s'est développé suite à l'avènement et à la massification des réseaux sociaux. Sur ces sites, le consommateur peut directement échanger avec une entreprise de son choix. Cela a pour avantage de faire remonter les besoins dudit consommateur mais est également une menace pour l'entreprise.

Ce concept, au départ marketing, réside dans le déploiement d'un système de veille permettant de surveiller ce que les internautes mentionnent au sujet d'une entreprise. Cette veille détecte les signaux faibles notamment via les réseaux sociaux. Ces signaux faibles aident l'entreprise à anticiper le mieux possible une attaque par le contenu ainsi qu'une action de contre-attaque.

Aujourd'hui, l'e-reputation répond à une prise de conscience des acteurs économiques. Ce concept est de moins en moins affilié au marketing et se caractérise par la mise en place de différentes tactiques au profit d'une stratégie d'entreprise. Pour preuve, la résonnance de ce terme se retrouve également au sein de l'Etat. Le Service de Coordination à l'Intelligence Economique a publié une fiche datant de Février 2012 intitulée « Protection de l'image de l'entreprise ».

Le personnal branding est l'image qu'une personne renvoie sur internet. En dehors du fait qu'il est nécessaire respecter ses engagements vis-à-vis de l'entreprise pour laquelle on travaille, lancer une attaque informationnelle sur des cadres peut être radicale. En effet, nuire à l'image d'un cadre c'est nuire à l'image de l'entreprise. Avec les réseaux sociaux dont nous parlions dans la partie précédente, il est d'autant plus aisé de compiler de l'information sur lui

[55] C. ALLOING, *E-reputation : vers une définition* »,CaddEreputation, overblog, 10/06/09.
[56] Ibid.

et de l'utiliser à des fins de polémique. Il sera également possible de créer des preuves via le contenant avant de lancer une attaque par le contenu

Les attaques mêlant contenant et contenu engendrent la complexification de ces attaques. Cette étape permet aux attaquants d'agir avec force et discrétion. La création de preuve par le contenant ainsi que sa propagation via le contenu ouvre la voie à une nouvelle forme d'attaque face à laquelle il est de plus en plus difficile à la fois de se protéger et de détecter le mensonge potentiellement latent.

L'exemple suivant nous montre qu'un nouveau type est possible : Un grand groupe français à été victime d'une attaque par le contenant visant à lier les adresses mail professionnelles de quelques une de ces cadres à un site pédophile avant de diffuser ce message via du contenu. La sécurité de l'entreprise est intervenue à temps pour faire échouer l'attaque[57].

Ce type d'attaque particulièrement redoutable et ne peut être anticipé que par l'humain. Aucun logiciel ne peut, pour le moment, parer à cette situation. D'où l'intérêt de contrôler les informations diffusées publiquement de la part de l'entreprise mais aussi de la part de ses employés.

[57] C. Harbulot, D. Lucas, *La guerre économique à l'ère de la société de l'information*, BDC AEGE, 2008.

Conclusion

La société de l'information a donc eu un impact considérable sur les rapports de force économiques et est devenue le théâtre de nouveaux types d'affrontements. Désinformation, atteinte à l'image, rumeurs, etc, les armes ne manquent pas et sont désormais utilisées en masse par nombre d'acteurs ayant cerné les enjeux de cette nouvelle donne stratégique.

La problématique est donc complexe et mal appréhendée. L'accent est trop souvent mis sur le contenant uniquement, les notions de cyberguerre et d'attaque informatique trouvant de l'écho aussi bien dans le grand public que chez les décideurs. Pourtant, force est de constater que l'attaque informationnelle, avec son potentiel destructeur, représente bel et bien une arme capable de mettre à terre une cible. La meilleure protection par rapport au contenant ne met pas à l'abri d'une attaque informationnelle, bien que cela permette de limiter certains risques.

L'aspect immatériel de la chose n'aide certes pas les entreprises à cerner le danger, bien que commencent à apparaître cellules de veille et référents en e-réputation au sein des grandes entreprises. Il est nécessaire de prendre en compte cette nouvelle donne stratégique en matière de guerre économique, tant les effets boules de neige peuvent être d'envergure[58]. Il est donc essentiel de veiller à décrypter les signaux faibles, prémices de ces attaques, de connaître ses propres vulnérabilités et d'avoir une politique d'entreprise à-même de répondre à ces dernières. Cette nouvelle sphère stratégique de l'information, et sa diffusion désormais virale, impose aux entreprises tant d'être à-même d'identifier leurs attaquants, leurs motivations, que d'être capable de se défendre de façon efficace. Cependant, cette défense ne pourra être pleinement efficace que si elle est soutenue par des dispositifs législatifs, quelque soit leur échelle d’application.

[58] Affaire Nestlé/Greenpeace, 2010.

Bibliographie

Ouvrages :

Général Alain de GAIGNERON, *Paix atomique et guerre révolutionnaire,* 1971

L. Gaildraud, C. Harbulot, *Orchestrer la rumeur, Rival, concurrent, ennemi… comment s'en débarrasser !*, Eyrolles, Paris, 2012.

C. Harbulot (dir), *Manuel de l'Intelligence économique*, collection Major, PUF, Paris, 2012.

C.Harbulot, D. Lucas, *La guerre économique à l'ère de la société de l'information,* AEGE, 2008.

C. Harbulot, *La main invisible des puissances*, Ellipses, 2007, Paris.

L. Gaildraud, C. Harbulot, *Orchestrer la rumeur, Rival, concurrent, ennemi… comment s'en débarrasser !*, Eyrolles, Paris, 2012.

O.Kempf, *Introduction à la cyberstratégie*, Economica, 2012.

Documents officiels :

ANSSI, *Stratégie de la France. Défense et sécurité des systèmes d'information*, Paris, février 2011.

Synthèse générale du groupe de travail sur les manipulations stratégiques dans le domaine économique et financier, Note du HRIE pour le 1er Ministre, 02/10/06

Rapport parlementaire sur les vecteurs privés d'influence dans les relations internationales, Assemblée Nationale, Paris, 2011

Revues et articles de presse :

AFP (source), *Le Ministère de l'économie et des finances victime d'une attaque informatique,* Journal Libération, 07/03/11.

M. Damgé, *Energie : un virus informatique frappe des sociétés du Golfe,* Le Monde.fr, 31/08/12.

Q. Domart, *« SNCF, la bataille du rail américain »,* Business International, 1janvier 2011

H. Guersmann, EDF fined EDF fined €1.5m for spying on Greenpeace, The Guardian, 10/11/11.

C. Haquet, *Qui sont les mercenaires de la cyberguerre*, L'express, 23/11/12.

Annie Kahn, Stéphane Lauer, «*Victime d'espionnage, Michelin s'interroge sur son culte du secret »*, Le Monde, Vendredi 28 octobre 2005

Didier Lucas, *« Les secrets des appels d'offres internationaux »*, Revue trimestrielle, Géoéconomie, Hiver 2009-2010

V. Marchive, *Air Liquide assure avoir échappé à Stuxnet*, LEMAGIT, novembre 2012.

Les démocraties occidentales faces à la guerre de l'information, La nouvelle revue géopolitique, 2011.

La cyberguerre. Autoscopie d'une menace, Dossier thématique, Lemonde.fr, 2004.

Les doux penseurs de la cyberguerre, Le monde, 1999.

Les guerilleros du web marketing, Le Monde, 31 janvier 2005

Le pétrolier Chevron a été infesté par le virus Stuxnet, Le Monde.fr, novembre 2012.

Plus de 460 hackers chinois arrêtés cette année, Le Monde, édition du 01/12/2010.

WikiLeaks : Pékin aurait commandité le piratage de Google, Le Monde, édition du 29/11/2010

Le déroulement de l'affaire Renault, L'Usine Nouvelle, 2011.

Articles publiés sur des blogs:
C. Alloing, *E-reputation : vers une définition »*, CaddEreputation, 10/06/09.
Les plus grosses attaques informatiques de l'histoire, Epercut Blog, 19/07/12.
S. Corre, *Contre-enquête sur une pseudo manipulation boursière via l'internet, ZDNet France*, 5 juin 2002
Guisnel, *Cyberattaques, l'appareil d'Etat visé à deux reprises*, Letelegramme.com,11/07/12.
Le Saumon, Document de présentation, Eurodecision-AIS, 14 mais 2004.
Amel Hammoum, *« l'affrontement ente LVMH et Hermes INTL »*, kwnockers.org, 13 mars 2012.
E. Protalinsky, *Anonymous attacks Ukrainian government after demonoid bust*, in *www.zdnet.com*, about 2012.
Cyber-opération sur le problème carbone, Knowckers.org, 14 mai 2012
Les activistes contre les ondes cherchent un nouveau bouc émissaire, Knowckers.org, 23 février 2011.
Quick en mode échec dans la guerre de l'information, knowckers.org, 20 mai 2011
L'Huile de Palme : la contre-attaque des producteurs, knowckers.org, 13 mars 2012
Relecture post Mortem d'une guerre de l'information (OPA Mittal contre Arcelor », Knowckers.org, 5 mars 2009.
L. Sinquin, B. Gosselin, D. Lucas, *Belvédère : résumé de l'affaire à destination des journalistes*, infoguerre, 23 Septembre 2009.

Base de connaissance AEGE[59] :
R. Ajlouni, *La république bolivarienne du Venezuela de Chavez VS le gouvernement américain de Bush*, BDC AEGE, août 2008
Z. Belkadi, C. Leon, C. Morishita, V. Navab, U. Randrianjatovo, L*a stratégie des entreprises du tabac face aux attaques informationnelles*, BDC AEGE, ESSEC, 27 avril 2007
O. Benazouz, M. Coulon, C. Renevot, M. Rougier, *Analyse et stratégie de riposte à la guerre informationnelle menée contre NSN/Siemens* BDC AEGE, 07/2009
Russie une opposition sous influence, Ecole de Guerre Economique, 8 juin 2012
O. Benazouz, C. Renevot, M. Rougier, *La guerre des ondes*, BDC AEGE, Décembre 2009
D. Devirgille, A.Harouna, I. Legay, T. Pitrat, R. Roulleaux Dugage , *Attaques sur le système financier Suisse*, BDC AEGE, 21 janvier 2010
S. Hautier, G. Gastaud, J. Laflèche, P-O. Kerbec, G. Le Pogamp, *Airbus / Boeing*, BDC AEGE, Mars 2005
E. Heurteux, A. Lubot, J. Hornung, A. Yassine, B. Traore, J-Y. Fargues, V. Mura, F. Miquel, R. Kaeppelin, M. Meunier, R. Moreau, Y. Regnier, A. Tanappa, *General Electric : Web ring dirty things to life*, BDC AEGE, Juin 2007
V. Le Masson, « *Carrefour remporte la bataille de l'opinion en Indonésie »*, BDC AEGE, 10 novembre 2011
Déstabilisation informationnelle des entreprises françaises en Argentine, Etude Etudiants de l'ESSEC, 2005.

[59] Documents produits par les membres du réseau AEGE.

La désinformation sur le lait, Mémoire étudiants de l'ESSEC, 2005
La guerre du lait, Etudiants de l'EGE, décembre 2009
La stratégie française d'IE en Afrique face au BTP chinois en Afrique, Etudiants de l'EGE, 2005.
Greenpeace et Nestlé : l'art de la guerre, BDC AEGE, 2010
La confrontation Suez-Véolia autour de la gestion de l'eau, ESSEC, 2007.
F. Miquel, A. Lubot, F. Vallee, V. Mura, B. Traore, *Le cas Sodexo aux USA*, BDC AEGE, 15 mai 2010
G. Mondrian, C. Harbulot, E*thique humanitaire et manipulation de l'information, BDC AEGE,* 6 septembre 2012
P. Teboul, *Les contradictions de l'amiante, le deuxième scandale,* BDC AEGE, Avril 2008
O. Thelot et F. Vallée, *Le parasitage informationnel du secteur arien : instrumentalisation de la nouvelle donne environnementale*, BDC AEGE, Juillet 2010

Sites internet :
www.cybercrimeswatch.com
www.ecommerce-infos.com
www.gartner.com
www.internetworldstats.com
www.opex360.com
www.wikipedia.com
www.zataz.com