

NOUVELLES MENACES, INFLUENCE ET CYBERESPACE

Depuis le 9 octobre dernier, date de la première séance commune aux quatre instituts désormais regroupés autour d'un pôle IHEDN/CHEAR et d'un pôle INHES/IERSE (bientôt élargi aux réponses pénales), les modalités d'application du rapport sur le renouveau de la pensée stratégique se sont enracinées dans le réel. Pour sa part, l'IRSEM (Institut de recherche stratégique de l'école militaire) regroupe désormais le secteur purement militaire, dans un cadre coordonné avec la mission de pilotage du projet général.

Grâce à l'investissement dynamique de la Présidence de la République,

du Premier ministre, des ministères de souveraineté, du CEMA... les travaux de construction des CHEM spécialisés (Intérieur, Affaires étrangères, Justice) sont lancés.

Au-delà des problématiques d'infrastructure, les réflexions sur les contenus, la démarche pédagogique, l'intégration des auditeurs précédents dans un outil de recensement des compétences ont largement avancé.

Il n'y a pas de fatalité à la crise mondiale de la pensée stratégique. Ce qui manque n'est pas la matière grise, mais la capacité à lui donner un cadre d'épanouissement permet-

tant de fournir à l'Etat et à la Nation, les moyens d'anticiper, de choisir, de gérer, de survivre aux crises.

Cette troisième édition, et dernière de l'année 2009, du supplément spécial de TTU marque l'importance des cybermenaces (qui ne remplacent pas les risques traditionnels, mais s'additionnent aux autres) et des nouvelles frontières de l'action du secteur privé dans une compétition mondiale de plus en plus poreuse aux activités malveillantes ou criminelles.

Alain Bauer, professeur de criminologie au CNAM

Stratégie, influence, image

L'élaboration de stratégies d'influence proprement dites constitue l'étape clé d'un authentique dispositif de sûreté. Pour le dire autrement, la communication d'influence recouvre l'ensemble des outils et actions visant à convaincre ou à dissuader les différents décideurs et/ou leaders d'opinion de rendre publique telle ou telle prise de position susceptible d'influencer positivement ou négativement la stratégie, les résultats ou le développement d'une organisation. Dans le cadre d'une compétition commerciale globalisée, force est de constater que les vainqueurs seront ceux qui réussiront à faire valoir leurs idées et leurs normes (qu'elles relèvent du droit «dur» ou de la «soft law»). Il est évident et fatal qu'un opérateur structure largement le marché en imposant ses références, ses normes techniques, juridiques ou culturelles : il ne lui reste plus dès lors qu'à proposer les produits qui répondent aux contraintes et besoins qu'il a lui-même contribué à façonner.

Mariant séduction et déploiement d'arguments rationnels, l'influence s'affirme comme un mode de per-

suasion offensif et se concrétise de différentes manières. Les acteurs du monde industriel peuvent ainsi construire des réseaux d'influence directe destinés à faire de «l'activisme» pour obtenir d'importants contrats. Ils peuvent également organiser des actions de lobbying auprès des instances internationales émettrices de normes (telle l'Union européenne). Les entreprises ont également la possibilité d'animer ou de soutenir des think tanks, universités, centres de recherche ou ONG dans le but de conforter un tissu relationnel favorable à leur positionnement sur le marché. Elles peuvent également créer ou participer à la dynamique de réseaux d'experts afin d'améliorer leurs connaissances ou de travailler leur image sur un domaine spécifique, s'affirmant par là-même comme un acteur de référence auprès des professionnels et des leaders d'opinion. Enfin, les entreprises peuvent organiser et conduire des programmes de social learning visant la préparation de la conquête de nouveaux marchés par la formation des élites.

Cependant, élaborer et mettre en œuvre une véritable politique de

valorisation d'image et de réputation ainsi qu'une communication d'influence optimale impliquent pour une entreprise d'acquiescer une vision de long terme dépassant l'échéance des résultats trimestriels, d'être capable d'identifier des courants médiatiques et intellectuels porteurs et de s'adapter aux nouvelles configurations de marché (lesquelles dépendent plus souvent qu'on ne le croit de facteurs extra-économiques). L'entreprise doit également être en mesure d'affirmer et de revendiquer sa propre identité.

Si l'on considère encore trop souvent l'influence sous un angle négatif, mettant l'accent sur la manipulation des faits, la désinformation, les excès ou dérives de certaines pratiques de lobbying, il faut pourtant répéter qu'elle constitue tout au contraire un moyen incontournable pour défendre et promouvoir ses intérêts à l'heure de la société de l'information et de l'économie de la connaissance. En ce sens, elle compose un élément clé de toute politique de sûreté globale et ambitieuse. (voir page 4)

L'INTERNET ET LE POLITIQUE

Le principe de la cyberguerre — avec la capacité pour des Etats, des entreprises ou des individus de mener sur la Toile des opérations offensives — a désormais largement progressé dans les esprits. Tant les états-majors que les opinions publiques se font peu à peu fait à l'idée qu'Internet constitue désormais un champ de bataille à part entière. Avec la possible prise de contrôle à distance de systèmes d'information stratégiques ou la manipulation des données accessibles sur le réseau des réseaux. Pourtant, ces interventions malveillantes sont loin de constituer les seules menaces émanant de l'Internet.

Quelle menace politique ?

Internet est tout sauf un écosystème déconnecté des réalités politiques du monde «réel». Ainsi, ce territoire représente un enjeu de rivalités entre les puissances. Qui s'y affrontent en maniant, notamment, l'arme juridique.

Alors que depuis 1998, date de création de l'Icann (Internet Corporation for Assigned Names and Numbers), cette association de droit californien exerçait, sous la tutelle exclusive du gouvernement des Etats-Unis, la gestion des noms de domaine ainsi que celle des treize serveurs racines sur lesquels repose l'architecture technique du Net, une décision prise par le Président Obama, fin septembre 2009, vient d'ouvrir une nouvelle ère. En effet, il a opté pour une remise en question de l'autorité des ministères états-uniens de la Justice et du Commerce sur l'Icann, au profit de quatre comités internationaux d'évaluation. Ils auront en charge l'examen des comptes de l'association, le respect de l'intérêt général, l'évaluation de la sécurité et de la stabilité des réseaux, les questions de concurrence et d'attribution des noms de domaine et le recensement des détenteurs desdits noms de domaine. Une fois levée cette mainmise sur l'Icann, se pose désormais la question de la répartition des pouvoirs entre les autres Etats de la planète. Soit, pour les mois à venir,

un terrain d'affrontements très prometteur... D'autant plus qu'au même moment, les parlementaires planchent à Washington sur un Cybersecurity Act of 2009 qui attribuerait, s'il est adopté en l'état, des pouvoirs considérables au Président des Etats-Unis en cas de «crise cybersécuritaire». Une latitude d'intervention allant par exemple jusqu'à la possible prise de contrôle par l'Exécutif des réseaux de communication détenus par le secteur privé.

Autre sujet de préoccupation pour les temps à venir : la question de la «neutralité de l'Internet». Selon ce principe, aujourd'hui encore en vigueur, l'accès de tous les internautes au réseau s'effectue dans les mêmes conditions de qualité. Sous la pression des industriels, notamment des opérateurs télécoms, cette règle fondatrice du Net tend à être discutée. Aboutissant ainsi à la discrimination technique de certains contenus, de facto rendus moins accessibles. Ce qui n'est pas anodin dans la société de l'information, où les contenus peuvent modeler des opinions publiques, des communautés d'individus...

Cette préoccupation de l'accès à l'information est également nourrie par le rôle grandissant des moteurs de recherche. Selon le cabinet de recherche ComScore, les internautes de l'ensemble de la planète ont rédigé en juillet 2009 plus de 113 milliards de requêtes par l'intermédiaire d'un tel moteur. C'est la première fois que la barre symbolique des 100 milliards a été dépassée. Puisque ce score a progressé de 41 % en une année. Leader incontesté : Google, qui règne sur 67,5 % du marché mondial. Le suivant, Yahoo, n'atteint même pas les 8 %. Le chinois Baidu vient ensuite à 7 %. Le filtre que constituent ces sites agit nécessairement sur la nature des informations récoltées par les internautes. Celui qui détient la clé de sélection des données, ainsi mises à la connaissance du public, est sans conteste un acteur politique, et évidemment économique, de premier plan. Même

si les comportements évoluent à grande vitesse : Facebook apparaît en dixième position des dix destinations qui génèrent le plus de requête. Dans la guerre de l'information, ces canaux doivent donc être pris en considération.

En matière d'intelligence économique, avec la possibilité offerte d'établir des cartographies précises et à jour des personnalités et de leur environnement professionnel, amical et familial, lesdits réseaux sociaux obligeamment mis en ligne sont de précieuses sources de renseignement. Là encore, ces données peuvent représenter un moyen d'approcher, dans les meilleures conditions, un individu considéré comme stratégique. Barack Obama en visite, début septembre 2009, dans une école états-unienne a ainsi conseillé à un élève qui lui demandait ce qu'il devait faire, dès à présent, pour un jour devenir, à son tour, Président des Etats-Unis, de commencer par faire attention à son profil sur Facebook et à ce qu'il mettait en ligne sur YouTube.

Enfin, le politique ne peut ignorer l'exploitation des systèmes d'information civils à des fins offensives. Il aura fallu attendre le mois de septembre 2009 pour que le Parlement européen adopte une résolution visant à exiger des garanties de la part du Conseil et de la Commission européens à l'occasion des discussions qu'ils mènent en ce moment avec les Etats-Unis sur l'accès de ce pays aux informations bancaires des entreprises et des citoyens européens. En effet, au nom de la lutte contre le terrorisme, Washington avait pris l'habitude de surveiller l'ensemble des transactions financières internationales, notamment via le système Swift. Le Parlement européen a ainsi reconnu que ce dispositif de surveillance pouvait être «utilisé abusivement pour pratiquer sur une grande échelle de l'espionnage économique et industriel». Un contrôle généralisé rendu possible grâce aux capacités de traitement des technologies de l'information... (suite page 3)

LA MENACE ÉCONOMIQUE

Quelle menace économique ?

La frontière entre menaces politiques et atteintes économiques est donc pour le moins ténue. Et le politique ne peut se désintéresser du secteur économique de la sécurité des systèmes d'information. Car, comme l'a écrit le préfet Daniel Canépa : «La sécurité d'un pays se mesure plus, aujourd'hui, en emplois sauvés et en domination économique qu'en victoire sur des champs de bataille.» Et Internet et la sphère technologique ne font certainement pas exception.

Le Président Obama ne dit pas autre chose quand, au printemps 2009, il annonce que son Administration travaillera «avec les acteurs clés du secteur — autorités locales et entreprises privées — pour apporter une réponse organisée et unifiée aux prochains cyberincidents (...) à l'instar de ce qui est fait pour faire face aux catastrophes naturelles». Il va même plus loin en indiquant alors que l'Exécutif «collaborera avec l'industrie pour trouver les solutions technologiques qui garantissent la sécurité et participent à la croissance». Soit une forme de partenariat public-privé particulièrement étroit auquel nous ne sommes pas forcément habitués de ce côté-ci de l'Atlantique. D'où l'intérêt de la démarche menée par exemple par l'Association française des éditeurs de logiciels (AFDEL) et le Syntec Informatique, qui souhaitent que l'industrie tricolore du logiciel puisse bénéficier des financements issus du grand emprunt national voulu par Nicolas Sarkozy. Un certain nombre de PME françaises très actives dans le domaine de la sécurité de l'information, comme le parisien DenyAll, le lyonnais Arkoon Network Security ou le nordiste Netasq, ont le potentiel technique pour devenir des acteurs importants sur ce marché. Encore faut-il qu'elles aient l'opportunité de le faire en conservant leur spécificité française. Car notre pays a besoin de détenir et de conserver une industrie de pointe en matière de sécurité des systèmes d'information. Ils font, à leur place, pleinement partie de la stra-

tégie globale de sécurité nationale. Leur mise en difficulté commerciale ou financière peut donc représenter une menace pour les intérêts français. Elle ne doit pas être sous-estimée.

Un management à risque

Au-delà des questions techniques et des enjeux high-tech, les technologies de l'information doivent également être envisagées sous un aspect très humain. D'une part, pour insuffler et diffuser une culture de sécurité au sein des organisations. Qu'il s'agisse d'entreprises, d'administrations ou de collectivités publiques. A l'occasion des Assises de la sécurité qui se sont déroulées à Monaco en octobre 2009, un Livre Bleu, précisément consacré à la culture du risque, a été publié. Avec une enquête menée auprès d'un panel de responsables des questions de sécurité.

Ces réponses sont éclairantes pour confirmer la diversité des situations et des approches. Et la nécessaire implication des «chaînes de commandement». Sans l'appui des directions générales et l'application au quotidien par l'ensemble des collaborateurs, le principe de sécurité — notamment en ce qui concerne les technologies de communication — risque de rester théorique. Des mesures de sécurisation imposées sans pédagogie préalable, des dispositifs si contraignants qu'ils sont rapidement ignorés par les utilisateurs finaux qui préfèrent s'y soustraire... les menaces sont nombreuses pour rendre une politique de sécurité inopérante dans les faits. Il est donc impératif d'imprégner les processus managériaux d'une dimension relative à la sécurité. Sans verser dans une paranoïa injustifiée, il serait salutaire que cette appréhension de la sécurité progresse. L'autre aspect de cette nécessaire prise en compte managériale sera la capacité prochaine des services de l'Etat, notamment la jeune Agence nationale pour la Sécurité des Systèmes d'Information (ANSSI), installée en juillet 2009 dans la continuité de la Direction centrale

de la Sécurité des Systèmes d'Information, jusqu'alors placée au sein du Secrétariat général de la Défense nationale (SGDN), à attirer et conserver des profils techniques pour mener à bien sa mission. Alors même que les entreprises privées ont, dans le même temps, leur marché pour se doter d'équipes de cybersécurité opérationnelles.

L'ANSSI compte aujourd'hui une centaine de collaborateurs et ses effectifs devraient au cours des toutes prochaines années passer à deux cent cinquante personnes. Il lui faudra développer des talents managériaux conséquents pour être pris en compte comme possible destination professionnelle par des candidats de valeur. Car le risque est grand que le passage, rapide, par une agence étatique soit perçu par un grand nombre d'entre eux davantage comme un moyen de valoriser un curriculum vitae que comme un choix motivé par le poste en lui-même. Une situation qui obligera l'Agence à gérer attentivement ses personnels contractuels. Pour éviter que le turnover rende difficile un travail de qualité sur la durée.

En parlant d'effectifs, on notera à ce propos l'annonce faite le 12 septembre 2009 par les autorités de Séoul de former quelque trois mille «cybergendarmes» d'ici 2010 afin de protéger les entreprises. Une décision qui fait suite aux attaques informatiques dont les intérêts sud-coréens ont été victimes en juillet 2009. Le but de cette formation à grande échelle d'experts civils ès-cyberguerres : «protéger les données des entreprises et empêcher les fuites de secrets industriels». Une réaction à la mesure du péril envisagé.

Nicolas Arpagian, rédacteur en chef de la revue *Prospective stratégique*. Coordonnateur d'enseignements à l'IERSE. Auteur notamment de «La Cyberguerre – La guerre numérique a commencé», Vuibert, 2009.

ENTREPRISES, SÛRETÉ ET CYBERESPACE

La société de l'information et ses technologies ont bouleversé l'environnement et le mode de fonctionnement des entreprises. Leur communication est devenue omniprésente et s'est même déplacée sur un nouveau terrain, à savoir la promotion de «valeurs», «principes éthiques» et comportements (ce que l'on regroupe dans la formule de Responsabilité sociale d'entreprise, ou RSE). A travers leurs produits et services, les firmes véhiculent un véritable style de vie et des modes de pensée. Mais rapidement, la société civile, et notamment les ONG, ont dénoncé la marchandisation des valeurs et ont initié, elles aussi, des jeux d'influence.

Certaines organisations, collectifs ou individus, orchestrent même des opérations de désinformation pour déstabiliser des entreprises, via la mise en cause de leur image ou/et de leur réputation. Ces dernières, faute d'anticipation, de préparation, se révèlent particulièrement vulnérables à ce type d'offensive. Les entreprises n'étant plus uniquement évaluées sur des critères financiers ou sur la maîtrise de savoir-faire techniques mais également sur des critères extra-économiques tels que leur comportement éthique, leur respect de l'environnement ou leur responsabilité sociale, il est évident qu'attaquer leur image revêt alors un intérêt stratégique.

Certaines firmes mettent en cause la réputation de leurs concurrents en utilisant les multiples instruments de la «guerre par l'information». Cette dernière vise à exploiter les

points faibles de l'adversaire en maniant l'art de la polémique et permet de mener des campagnes de déstabilisation informelles le plus souvent licites, même si le fair play s'en trouve offensé. Toutefois, certaines pratiques conduisent carrément à des dérives, notamment lorsque l'information se voit littéralement manipulée ou que le public est clairement désinformé. En octobre 2000, Alcatel a vu son action plonger de 10 % suite à la publication de faux communiqués de presse. Le groupe Total a quant à lui été victime, au moment du drame de l'«Erika», de la diffusion de photos truquées et de fausses correspondances internes.

Maîtriser le risque informationnel

Force est donc de constater que la gestion du risque informationnel est une composante de la sûreté des entreprises. Mais qu'entend-t-on par risque informationnel, ou plus exactement par risque d'atteinte à l'image ? Ce dernier se définit comme la résultante des conséquences potentiellement nocives pour un acteur de la médiatisation, orientée ou non, d'informations stratégiques, réelles ou manipulées, le concernant ou l'«impactant». En effet, en affectant ponctuellement ou durablement l'image, la stratégie et les performances de l'entreprise, le risque informationnel peut remettre en cause la pérennité de l'entité ou son développement. La maîtrise de ce risque s'effectue tout d'abord par la mise en place d'un dispositif spécifique de prévention et de protection. L'entreprise, après avoir

identifié ses vulnérabilités informationnelles, doit élaborer un plan de veille afin de cartographier les acteurs susceptibles d'utiliser ses failles ou de manipuler des informations pour nuire à ses intérêts. Il s'agit ensuite d'imaginer et de hiérarchiser les arguments que ses adversaires pourront utiliser. A ce stade, des contre-argumentaires devront être élaborés. Parallèlement, la firme s'attachera à réduire l'occurrence et la gravité du risque en traitant les dysfonctionnements de tous ordres susceptibles d'être instrumentalisés. La maîtrise du risque informationnel s'effectue en dernier lieu par un pilotage «fin» de la communication de l'entreprise et de son exposition médiatique (notamment par l'intermédiaire de ses principaux dirigeants : la stratégie médiatique choisie par Jean-Marie Messier, à l'époque où il présidait aux destinées de Vivendi, rendit, par exemple, plus délicate la politique de communication du groupe). De la même manière, si l'on peut débattre longuement de la pertinence économique des «parachutes dorés», il est manifeste que cette question affecte l'image de certaines entreprises en période de crise. Concrètement, si la sûreté d'un groupe ou d'une grosse PME implique une stratégie de traitement du risque informationnel visant à promouvoir la réputation de l'entité auprès de l'ensemble des parties prenantes, le premier objectif de cette dernière est d'assurer la cohérence des différents messages (explicites ou implicites) diffusés.

Eric Delbecque,
directeur de l'IERSE

**CE NUMÉRO SPÉCIAL EST PUBLIÉ AVEC LE SOUTIEN D'AB ASSOCIATES,
CONSEIL EN SÉCURITÉ GLOBALE.**