1° Juillet 2010

Dernier épisode du conflit qui oppose la Chine et Google : ce dernier a du avouer sur son blog qu'il cessait de rediriger les demandes d'internautes chinois vers Google non censuré de Hong Kong.

En effet, il doit renouveler - comme tout site ayant une activité en Chine- sa licence annuelle auprès du ministère de l'Industrie et des Télécommunications. Lequel a fait comprendre à la société californienne qu'il fallait mettre fin à ce routage provocateur. Et comme la demande de Google est parvenue "tardivement", Pékin se laisse toujours la latitude de sanctionner Google sous un prétexte administratif. La principale communauté d'internautes au monde qui n'a plus d'accès à Twitter, à Facebook ou à You Tube (les autorités chinoises ont tiré les conséquences du précédent iranien) pourrait être réduite à faire ses recherches sur le moteur national, Baïdu (déjà bien plus utilisé là-bas que Google). Sinon, un internaute parlant chinois et faisant depuis la Chine continentale une recherche par mots clés avec le plus grand moteur de recherche de la planète passera forcément par un système de filtres. Il l'empêchera par exemple d'aller sur les sites de la secte Falun Gong ou celui d'opposants à la présence chinoise au Tibet.

Ce qui équivaut à un retour à la situation d'il y a quatre ans. À l'époque, l'opinion avait découvert que les moteurs de recherche comme Google (mais aussi Yaho ou MSN) étaient censurés en Chine . Pour reprendre un exemple célèbre, c'était pratiquement le seul pays où l'on ne pouvait pas trouver de photographies des événements de la place Tien An Men sur la Toile.
Les leçons de l'affrontement Google/Chine, commencé cette année quand Google a menacé de se retirer d'un pays qui espionnait les comptes mails des pro-tibétains, se confirment :
- par une savante combinaison de censure, de surveillance des points d'accès (pas d'anonymat dans les cybercafés), de gestion des fournisseurs d'accès, d'obligations légales (par exemple celles qui touchent à l'identité des responsables de sites) et de négociations avec les Occidentaux alléchés par le plus grand marché numérique du monde, on peut faire ce que les prophètes d'Internet disaient impossible : contrôler l'information numérique à laquelle ont accès plus d'un milliard de gens, les isoler numériquement du reste de la planète et pourtant développer une économie numérique de pointe.
- pour le dire autrement : le politique n'est pas si désarmé face au technologique.
- la stratégie de Google (avec son slogan moraliste "*Be no evil*") même soutenu par la politique de diplomatie publique d'Hillary Cliton (prête à soutenir toutes les dissidences sur Internet) se heurte au mur de la puissance et de l'autorité.

L'utopie d'une multinationale faisant céder une grande puissance par la menace de se retirer et de la priver de sa technologie s'éloigne autant que celle d'une Toile par nature rebelle à toute censure.

30 avril 2010

De récentes révélation du New York Times jettent un nouvel éclairage sur l'affaire Google contre Chine, plusieurs fois traitée ici. Comme on s'en souvient, Google, sans exécuter à proprement parler sa menace de quitter le pays en avril, avait décidé fin mars de détourner les requêtes faites à son moteur de recherche de Chine continentale vers celui de Hong Kong, en principe non censuré. Se plaçant ainsi délibérément sur un plan de libertés publiques et militant pour le droit des internaute à une information non contrôlée par le gouvernement, Google publie par ailleurs un palmarès des États qui censurent la Toile. Plus exactement une liste des gouvernements qui lui demandent de rendre inaccessibles des données (des vidéos sur You Tube par exemple) ou d'espionner des Internautes.

Surprise : les premiers de la liste sont le Brésil (en tête et pour les demandes de retrait et pour les demandes d'information sur les utilisateurs), l'Allemagne et les États-Unis, donc pas les trois pires dictatures de la planète. Ainsi, le pays de Lula présente par 3.663 requêtes d'information sur des internautes à Google, les États-Unis 3.580 et la Grande-Bretagne 1.166. La France est au cinquième rang avec 846 demandes. À la rubrique Chine, Google mentionne simplement : "Les responsables chinois considèrent que les demandes de censure relèvent du secret d'État aussi ne pouvons-nous révéler cette information pour le moment". Et comme Pékin prépare, de son côté, des lois renforçant le secret d'État et permettant de mieux contrôler Internet, on ne peut pas vraiment dire qu'un ouragan libertaire balaie l'Empire virtuel du Milieu.

La mesure anti-censure décidée par Google a-t-elle été efficace ? On n'a guère vu ses concurrents se précipiter vers la sortie ni jouer la carte de la résistance face à Pékin. Comme c'était prévisible, le déplacement du moteur Google (ce qui permet facilement aux autorités chinoises de réguler les flux de demandes vers Hong Kong) a plutôt profité à Baïdu son rival chinois officiel, qui, lui, ne fait rien - et pour cause - qui puisse gêner les autorités : son résultat augmente de 165 % (70,4 millions de dollars au premier trimestre), le chiffre d'affaires progressant de 60 %, à 189,6 millions de dollars.

L'initiative de Google n'a guère été relayée non plus. Au moment où s'ouvre l'exposition universelle de Shangaï, superbe opération de diplomatie publique, on n'entend plus guère parler du fabuleux facteur d'ouverture que serait la présence de millions d'étrangers, dotés de téléphones et d'accès à Internet, comme cela se disait avant les jeux olympiques de Pékin. Et après le discours d'Hillary Clinton plaçant la liberté de naviguer sur Internet au nombre de principales libertés que les USA devaient défendre, les gouvernants qui font le voyage de Chine reprennent pour le moins discrètement le thème de la fin de la censure.

Tout ce qui précède n'a de sens que si l'on se place dans la perspective d'un combat des partisans des droits de l'homme (en l'occurrence Google) contre un État autoritaire : après tout, ce qui avait déclenché tout cela, est la révélation par la firme californienne que des comptes de courriel en particulier ceux de dissidents pro-tibétains avaient été piratés et que les attaques venaient de Chine (certains avaient même pointé deux adresses Internet correspondant à deux centres de formation chinois en informatique).

Dès le début, l'affaire avait été pourtant été passablement embrouillée : Google, lorsqu'il se référait aux "attaques informatiques" subies depuis la Chine en décembre 2009, parlait à la fois de tentatives d'intrusion dans les systèmes d'importantes sociétés et de pénétration dans les comptes de particuliers (dont de supposés partisans des droits de l'homme).

Le tout recouvrant une troisième réalité : à savoir le fait que les demandes des internautes chinois au premier moteur de recherche du monde étaient filtrées à la demande des autorités.

Pour en revenir aux révélations du Nex York Times, si elles étaient confirmées, elles nous apprendraient ceci : selon "*une personne ayant une connaissance directe de l'enquête*" (dixit le NYT), l'attaque portait en réalité sur un système de mots de passe, surnommé Gaia. Il contrôle l'accès de millions d'internautes à travers le monde à plusieurs services de Google (y compris des services d'affaire et, accessoirement, des comptes e-mail). Les pirates, qui semblaient avoir ciblé des développeurs de Google et ne connaissaient précisément le nom, auraient eu accès aux codes sources du programme en Californie. Google s'est contenté de déclarer qu'il renforçait la sécurité de Gaia, sans que personne puisse établir définitivement le degré de gravité du dommage subi ni surtout du dommage futur. Les pessimistes décrivent les intrus comme désormais capables de percer les secrets de fabrication de Google et surtout ses failles de sécurité. Les voleurs auraient-ils dérobé "les bijoux de la couronne", ou plutôt les clefs de la maison. Croit-on sérieusement qu'il n'y a derrière tout cela que des policiers chinois violant la correspondance numérique des amis du dalaï-lama pour mieux les réprimer ? Au-delà du débat techniques, qui concerne seulement quelques experts, il semble de plus en plus évident que nous soyons en face d'une gigantesque affaire d'espionnage industriel recouverte par les brumes d'une phraséologie morale.

1° Avril 2010

L'IRIS LANCE L'OBSERVATOIRE GEOSTRATIQUE DE L'INFORMATION

Sous la direction de *François-Bernard Huyghe* et d'*Eddy Fougier*, chercheurs associés à l'IRIS, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Notamment les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

1er DOSSIER : LA CHINE ET GOOGLE, DÉCRYPTAGE D'UN CONFLIT

Dossier dirigé par *François-Bernard Huyghe*

« Deux tigres ne peuvent pas vivre sur la même montagne » : l'affrontement de deux modèles - Par Fabienne Clerot, chercheur associée à l'IRIS

Guerre de l'information et cyberguerre en Chine - Par Daniel Ventre, ingénieur au CNRS

Google Is Go(o)d - Par Stéphane Charrière, co-fondateur de l'Observatoire Alterbrand

Google dans son plus simple appareil - L'entreprise la plus forte du Monde - Par Olivier Jeandel, ingénieur spécialisé en développement de projets internet

Deux leçons stratégiques de la crise Chine Google - Par François-Bernard Huyghe, chercheur associé à l'IRIS

Rappel des faits en quelques liens - Glossaire -

LE DOSSIER -

TÉLÉCHARGER

Deux leçons stratégiques de la crise Google Chine

1°) Technologie et idéologie sont inséparables

Certes, l'affrontement impliquant Google, les gouvernements chinois et américains, peut-être des groupes privés de pirates informatiques, sans doute des grandes sociétés US (et, dans tous les cas, jouant de l'opinion des internautes) portait sur des questions techniques :

- l'efficacité et la traçablité d'attaques informatiques (donc la possibilité de prouver l'identité de leurs auteurs)
- la capacité d'un État, à l'heure de la mondialisation numérique, de fermer ses frontières aux influences venues de l'extérieur via Internet, sa volonté de censurer ses propres internautes, éventuellement d'espionner ou de saboter à distance des systèmes informationnels d'autre pays
- la nature, la probabilité et la gravité d'une éventuelle cyberattaque entre grandes puissances
- le degré d'autonomie technologique que peut acquérir un État souverain dans un monde en réseaux (concrètement :peut-on «se passer» de Google, de Faceboolk ou de Twitter et être un pays en plein développement économique et technique ?)

Mais au-delà de ces questions de technologie, d'ailleurs encore mal résolues, se sont vite révélés des positions idéologiques : Celle de la Chine n'est une surprise pour personne : les autorités sont toujours décidées à concilier système économique mondialisé et contrôle politique de la population (donc des moyens de communication). Quitte à jouer sur la fibre nationaliste, Pékin veut à la fois affirmer sa fermeté, sauver la face face devant tout ce qui ressemblerait à une pression de l'étranger et assurer au maximum son autonomie

technologique.
D'où l'emploi de moyens régaliens (y compris sans doute ceux clandestins de l'espionnage) dans la guerre économique planétaire. Google est apparu comme un acteur «idéologique» dans la mesure où, après s'être compromise en 2006 en acceptant de censurer son moteur de recherche en Chine continentale, la compagnie a joué à fond la carte du capitalisme moral, défendant les droits de l'homme contre ses intérêts apparents (apparents car la perte d'un chiffre d'affaire de 300 millions de dollars, une pécadille pour le géant, est peut être plus que compensée en bénéfices politiques et publicitaires).
Le refus proclamé de se rendre complice de régimes autoritaires au nom du réalisme économique est probablement conciliable avec une stratégie de développement à long terme. Reste pourtant qu'aux yeux de millions d'internautes, c'est une société privée qui se porte à la pointe du combat pour les libertés en Chine, non un acteur politique. Il est d'ailleurs stupéfiant de voir une multinationale menacer une super puissance, poser des exigences politiques, provoquer les autorités chinoises (en cessant de respecter l'accord sur la censure de son moteur de recherche, Google les pousse à le chasser ou à le réprimer). Mais aussi précéder les autorités de son propre pays (au moins en paroles) et coopérer ostensiblement avec la *National Security Agency* pour identifier les auteurs des attaques subies depuis le territoire chinois (ce qui n'est pas une preuve formelle que les services chinois soient impliqués).
L'administration Obama a retrouvé ses réflexes démocrates du temps de Clinton et des discours d'Al Gore sur l'agora électronique planétaire : défense des libertés et aide à toutes les dissidences pour renforce son *soft power* d'influence, volonté de promouvoir une société planétaire de l'information sur le modèle américain, inséparable de la démocratie pluraliste et du marché, confiance dans les technologies «libératrices». Tels furent du moins les thèmes d'un discours d'Hillary Clinton du 21 janvier plaçant la liberté universelle de se connecter sur le même plan que les autres grandes libertés qu'incarnent les USA. Dans un affrontement avec le rival économique chinois, l'arme de la subversion démocratique n'est pas négligeable.

2°) Surveillance, espionnage, guerre : le conflit devient multidimensionnel.

Le plus significatif dans cette affaire est sans doute que nous avons de plus en plus de mal à distinguer des catégories d'action autrefois bien distinctes :
- la surveillance qu'exerce un État souverains sur les communications de ses citoyens via la censure établie par la loi, le repérage policier des éléments dissidents et éventuellement la fermeture de leurs moyens matériels de s'exprimer
- l'espionnage économique, même pratiqué à distance, pour s'emparer des secrets d'un concurrent et anticiper sa stratégie.
- le sabotage qui consiste ici à contrôler ou altérer les moyens de communication d'un rival et d'un adversaire en dehors de son propre territoire national
- la guerre (fut-elle baptisée «cyberguerre») qui n'est pas un mot à employer à la légère. Les «cyberattaques» qui sont à l'origine de toute cette affaire et que Google a dénoncées dès le 12 janvier présentent en effet plusieurs caractéristiques. Elles étaient anonymes (au mieux, on pouvait en retracer l'origine jusqu'à des adresses IP situées sur le territoire chinois). Si certaines portaient sur des comptes e-mail de supposés militants des droits de l'homme, d'autres, de haut niveau technique, touchaient de grandes firmes.
Elles combinaient des capacités d'infiltration et de prise de contrôle à distance sur d'autres machines, capacités qui pourraient tout aussi bien servir à prélever des données confidentielles qu'à empêcher le fonctionnement d'un système informationnel. Donc à violer

des secrets mais aussi à produire un ravage et un effet de chaos et désorganisation. Donc éventuellement pouvant servir un dessein militaire. Enfin et surtout, dans toute cette affaire, la victime ne sait jamais (ou ne peut jamais démontrer) qu'elle est attaquée par un acteur étatique (seul susceptible en principe d'accomplir des actes de guerre), par un groupe criminel privé, ou par des militants animés par une motivation idéologique et politique (comme des «hackers patriotes»).

Au total, les frontières entre militaire, politique, criminalité économie et technologie ont été constamment remises en cause. Derrière les proclamations théâtrales, les nouvelles formes d'une conflictualité insaisissable, hors frontières et hors limites, envahissant tous les domaines. et qui pourraient bien redéfinir de grandes stratégies de puissance.

24 mars 2010

Le conflit entre l'Empire du Milieu et la Société du Bien rentre dans une nouvelle phase. Google (dont la devise est "*be no evil*") après avoir annoncé son intention de se "retirer" de Chine au nom des droits de l'homme qui y sont toujours bafoués, vient, plus subtilement, de provoquer Pékin : il a détourné son moteur de recherche google.cn. vers celui de Hong Kong, également en chinois mais non censuré.
Le but est évidemment d'obliger les autorités à réagir et à prendre publiquement leurs responsabilités, soit en censurant elles-mêmes les recherches des leurs internautes (et l'on verra bien alors qu'il s'agit de dissidence, pas de protection contre la pornographie), soit en fermant le moteur de recherche qui est consulté par 90% des internautes de la planète (mais seulement, il faut le préciser par environ un tiers des 384 millions d'internautes chinois).
Du reste, Pékin vient d'annoncer des rétorsions et de baisser le débit de la circulation en direction du site de Hong Kong. China Mobile et China Unicom ou encore Top.Com viennent d'abandonner des projets juteux avec la compagnie américaine. En attendant d'autres mesures.
Mais comme l'a dit Mr. Drummond le représentant juridique de Google : "*It is good for our business to push for free expression*," (c'est bon pour les affaires de se battre pour la liberté d'expression).
Google aurait donc donc révélé le hideux visage de la dictature qui prive ses citoyens du droit à l'information et à l'expression. Et chacun de se persuader qu'il s'agit d'une question de libertés publiques et uniquement de cela : la Chine pourra-t-elle maintenir un chape de plomb à l'heure de la communication planétaire ?
À première vue, il s'agirait donc d'un conflit, certes à prétexte commercial, mais surtout politique et éthique. Il opposerait d'une part une compagnie qui avait certes péché autrefois en acceptant de censurer la version locale de son moteur de recherche, mais qui vient de reprendre une posture morale en refusant de se rendre complice plus longtemps, exemple à ceux qui seraient tentés de s'implanter en Chine au prix de compromis. Et d'autre part, un pouvoir archaïque uniquement soucieux de contrôler ses citoyens.

Certes, quelques mauvais esprits font remarquer que, dans cette affaire, Google dont le chiffre d'affaire s'élève à 24 milliards de dollars, ne perd *que* 300 millions dans un pays où, de plus, il est largement dépassé par le moteur local Baïdu. La perte provisoire d'un marché pas si rentable sera peut-être largement compensée par l'opération publicitaire qu'ont réalisé Brin et Page, les jeunes dirigeants de la firme : désormais leur logo sera synonyme de libertés. Et des générations de jeunes internautes seront moins tentées de la critiquer pour sa position hégémonique ou pour l'exploitation commerciale qu'elle fait des données personnelles.
Les Occidentaux qui espèrent prendre les parts de marché de l'entreprise californienne (comme Microsoft avec son moteur Bing) pourraient bien ne faire qu'un calcul à court terme.
Il y a peut-être du vrai dans cette hypothèse, mais là n'est pas l'essentiel. S'agit-il uniquement d'une affaire de censure et de droits de l'homme ? Ou d'autres enjeux stratégiques sont-ils en cause ?
Depuis le début de cette affaire - c'est à dire depuis la déclaration de Google du 12 janvier se plaignant d'attaques informatiques, il existe une ambiguïté sur ce qui est vraiment reproché aux Chinois ; les premières déclarations faisaient état de deux sortes d'intrusions venues de Chine (par "venues de Chine" nous entendons dont l'origine peut apparemment être tracée jusqu'à des adresses IP situées sur le territoire chinois, ce qui n'est pas la preuve que l'État chinois les ait provoquées, qu'il en soit la source, voire même qu'il les ait connues et tolérées).

Il y avait d'une part des attaques (selon les versions données par la presse "très sophistiquées", "très simples et utilisant des techniques de tromperie de type phishing" ou encore "reposant sur des complicités humaines à l'intérieur de Google") et qui portaient sur la confidentialité du courriel d'un certain nombre de gens (possesseurs de comptes Gmail offerts gratuitement par la compagnie), dont des militants des droits de l'homme. Et puis, il y avait une seconde attaque portant, elle, sur sans doute trente compagnies américaines, dont Adobe, Northrop Grumman et Dow Chemical pour des raisons qui ont certainement peu à voir avec la secte Fanlun Gong ou les démocrates de la place Tien An Men.

Or très curieusement, tout le monde semble oublier ce volet, qui ressort visiblement de l'espionnage industriel de haut niveau, pour ne se consacrer qu'au dossier plus gratifiant des droits de l'homme (il permet de se positionner dans le camp du bien sans discussion possible).

Pour le dire autrement, il y a deux questions dont la première tend à occulter la seconde :

1) La Chine a-t-elle le désir de contrôler politiquement toute forme de dissidence potentielle sur le Net, tout en permettant à sa population d'utiliser un instrument indispensable de développement économique ? En ce cas en a-t-elle les moyens techniques, contrairement à tout ce qui s'écrit depuis des années sur le forum planétaire et la technique libératrice (les technologies de la communication supposant automatiquement une société ouverte) ?

Outre les moyens de contrôler les internautes chez les fournisseurs d'accès ou sur les moteurs de recherche, outre son action répressive et sa capacité d'interdire d'accéder à certains des services les plus connus d'Internet comme Twitter et Facebook, Pékin peut-il recourir à des moyens de surveillance efficaces pour repérer d'éventuels dissidents numériques ? Il est évident qu'il faut répondre oui à toutes ces questions.

2) La Chine, conformément à ce qu'écrivent certains de ses stratèges, est-elle en train de se doter d'une capacité de mener des cyberattaques de haut niveau ? Ces attaques prennent elles pour le moment la forme de pénétration dans des systèmes stratégiques pour s'emparer d'informations précieuses (autrement dit : cyberespionnage) ? Peuvent-elles prendre demain la forme d'attaques capables de paralyser de systèmes d'information ayant une valeur stratégique de type militaire, mais aussi économique et technique (autrement dit : cybersabotage) ? Est-ce cela qui inquiète non seulement Google, mais aussi l'administration Obama ? au point qu'Hillary Clinton a relancé une sorte de "cyberguerre froide" numérique en présentant les USA comme menant la croisade planétaire pour la technologie électronique libre et libératrice ? Là aussi nous sommes tentés de répondre oui. Le jeu à trois Chine / Google / USA mérite visiblement des analyses un peu plus approfondies et d'autres expertises. C'est pourquoi nous invitons les visiteurs de ce site à se rendre dans quelque jours sur celui de l'IRIS et à suivre les travaux du tout nouvel *Observatoire géostratégique de l'information* qui consacrera ses premières recherches à ce sujet.

23 Janvier 2010

L'affaire de la cyberguerre opposant la Chine à... - à qui au fait ? à Google, à des activistes tibétains, aux USA, au reste du monde ? - est en train de monter en puissance.
Derniers développements de ce que certains ont baptisé "opération Aurora" :
- Après ses menaces des premiers jours, Google négocie maintenant avec Pékin, y compris, semble-t-il, sur l'enjeu que représenterait éventuellement le maintien d'une censure sur son moteur de recherche version chinoise.
- Les autorités chinoises ont réaffirmé leur volonté de contrôler Internet (sous les habituels prétextes de lutte contre la pornographie et le piratage) tout en faisant des appels aux sociétés étrangères qui auraient pu être découragées par ce qui semble surtout être un beau cas d'espionnage industriel (éventuellement doublé d'une volonté de surveiller les dissidents)..
- Baidu, le moteur de recherche chinois rappelle qu'il a été lui aussi victime de cyberattaques, en particulier d'une certaine Cyberarmée iranienne qui s'était déjà attaquée à Twitter (on comprend pour Twitter qui avait largement servi à l'opposition iranienne à dénoncer la répression hors de ses frontières, mais pourquoi taguer en persan un portail chinois ?). On notera au passage que la Chine ayant le plus grand nombre d'internautes au monde (certaines estimations font état de 384 millions), il n'est pas illogique que ce pays soit aussi la première réserve potentielle de hackers voire aussi de victimes de la cyberdélinquance.
- Enfin et surtout, tout en demandant des explications à la Chine sans vraiment l'accuser, Hillary Clinton vient de prononcer un important discours sur la question de la liberté sur Internet, texte où la célèbre revue Foreign Policy voit l'amorce d'une cyberguerre froide. Il fait suite à plusieurs mises en cause des anciens ennemis de l'Est dans des cyberattaques (de l'été 2009, de fin 2008, etc.), et fait écho aux nombreuses mises en garde par des centres derecherche sur le danger chinois dans le cyberespace. Mais cette fois, Mrs. Clinton lance plusieurs thématiques idéologiques en présentant les USA comme les défenseurs planétaires d'une liberté sur Internet, comme ils le furent "dans le monde réel" à l'époque du rideau de fer.
- Tout tourne autour du thème sur lequel Clinton (Bill, le président) et Al Gore avaient joué en leur temps : celui de la grande agora planétaire et la célébration de la société globale interconnectée par la Toile "comme par un réseau nerveux". Internet est envisagé à la fois comme un outil de bonne gouvernance, un stimulant de la créativité donc une source de richesse et un moyen de contrôle démocratique. La circulation des flux d'information irait dans le sens historique d'un élargissement du modèle américain : transparence, initiative citoyenne, démocratie pluraliste, marché, libre initiative et société de l'information. Vieux discours utopique qui est ici recyclé, y compris avec son bémol inévitable : il y a une rançon à tant de bienfaits et un risque pour tant d'opportunités : les tentatives de censure les gouvernements autoritaires, les "discours de haine" comme ceux d'al Qaïda et le détournement de la technologie libératrice vers de mauvais usages : " Les technologies qui ont le potentiel de donner accès au gouvernement et de promouvoir la transparence peuvent aussi être détournées par les gouvernements pour écraser la contestation et attenter aux droits de l'homme".
Les États-Unis, dans la tradition de Roosvelt qui voulait promouvoir les quatre grandes libertés (d'expression et de culte, mais aussi la libération du besoin et de la crainte) auraient donc pour mission de reprendre le combat de libération adapté aux potentialités de la technologie à l'ère numérique.
Le nouveau mur de Berlin, ce serait la censure d'Internet, les nouvelles persécutions religieuses, celles qui frappent les bloggers dans des pays intégristes comme l'Arabie

Saoudite. La libération du besoin passe par l'accès à l'éducation par les réseaux. Quant à la libération de la crainte, elle supposerait la sécurisation d'Internet (y compris pour le commerce électronique et la protection de la propriété intellectuelle) et la lutte contre le cybercrime ou les cyberattaques. Et Hillary Clinton de faire l'apologie d'une cinquième liberté fondamentale, garante des quatre premières : celle de se connecter.

Que signifie en pratique ce discours libéral- technophile ? Concrètement, l'annonce que les USA font faire tous leurs efforts diplomatiques, économiques et technologiques pour développer cette grande interconnexion planétaire, doublement bénéficiaire et pour les libertés dans le monde et pour les intérêts du pays qui est à la pointe de la nouvelle vague historique.

L'aide aux dissidents empêchés par leur gouvernement d'avoir accès à la Toile est à l'ordre du jour (reprenant et réadaptant cette fois la tradition de "diplomatie publique" du temps de *Radio Free Europe*). Le gouvernement américain s'impliquerait même dans la coopération avec les privé pour développer de "bonnes technologies" (Mrs. Clinton donne pour exemple des logiciels pour téléphones mobiles qui permettraient aux citoyens de "noter" leurs gouvernants en termes d'efficacité, transparence, corruption...) : donc coopérer avec des individus ou des compagnies (Microsoft est cité) pour "des idées et applications qui pourraient contribue à nos objectifs diplomatiques et de développement". Le software au service du softpower !

Il s'agirait aussi d'inciter les sociétés américaines à tenir davantage compte du facteur des libertés dans des négociations avec le pays où elles veulent étendre leurs activités. Traduction : les USA ont l'intention d'utiliser l'arme économique, là aussi dans la tradition de l'advocacy center créé par Bill Clinton pour promouvoir la stratégie d'influence nationale à travers la coopération entre l'État et ses entreprises stratégiques. Pas de technologie américaine sans contrepartie politique pour les gouvernements qui veulent faire du business.

Il s'agirait en somme "d'aligner nos principes, nos buts économiques et nos priorités stratégiques" : business + droits de l'homme + intérêt national. Décidément, c'est bien la remise à jour de la stratégie d'*enlargment* des années 90, sous le nouveau slogan de "21st century statecraft", des outils politiques du XXI° siècle. Un nouveau sens de l'Histoire - conférant un rôle d'avant-garde aux USA - mais qui se marquerait plus tôt à travers le développement de Twitter et de Facebook est ainsi appelé au secours d'une politique d'influence qui compte bien utiliser le levier de l'idéologie et de la technologie face à ses concurrents. L'administration Obama un peu essoufflée en ce moment semble lancer là une nouvelle thématique bien dans une certaine tradition "wilsonienne" démocrate. Et l'affaire chinoise pourrait bien servir de déclencheur à une grande offensive politique US. Affaire à suivre...

18 janvier 2010

Une cyberguerre entre la Chine et... Google ? Superpuissance contre méga-entreprise ? Cette surprenante nouvelle qui circulait dans la presse vers le milieu de Janvier 2010 mérite un examen un peu plus attentif.

Nous avons suffisamment critiqué le terme de cyberguerre ici pour nous méfier de son emploi médiatique : une guerre sans morts, sans armées, sans différence réelle entre civils et militaires (que ce soit côté acteurs ou côté cibles), sans paix ni traité, sans territoire précis, sans buts politique clairement discernables et qui soit destiné à s'inscrire dans l'Histoire (comme l'annexion d'un nouveau territoire), etc. peut-elle être vraiment qualifiée de guerre ? Certainement pas au sens de Clausewitz ou du droit de la guerre traditionnel.

La cyberguerre, plus souvent évoquée par les stratèges que vécue par des "combattants", pourrait préparer, relayer, amplifier et certains disent même peut-être remplacer, l'action des forces armées par des attaques électroniques contre des dispositifs militaires, étatiques (politiques ou administratifs) mais aussi privés. Ainsi, le Livre Blanc de la Défense Nationale mentionne la "guerre informatique" parmi les problèmes de la sécurité nationale, affirmant que notre pays doit se doter de moyens de contre-offensive (et pas seulement d'outils de défense et de sécurité), ce qui suppose une doctrine d'emploi. À défaut de guerre, il existerait donc au moins des cyberattaques, menées par l'intermédiaire du Net, produisant des dommages sur des cibles civiles ou militaires.

Leur dangerosité pourrait résulter
- soit du désordre qu'elles provoquent ou provoqueraient (paralyser tout un pays dépendant de ses réseaux informatiques, au moins créer du chaos dans des infrastructures dites vitales comme des aéroports, des banques, des systèmes d'approvisionnement électronique...). Donc essentiellement des attaques contre des systèmes
- soit en s'emparant d'un patrimoine informationnel précieux ou de données stratégiques qui devraient en principe être secrètes et protégées par un État souverain. Ce qui ressemble singulièrement à de l'espionnage.
- soit en recherchant un certain impact psychologique sur les décideurs ou la population, en effectuant des actions de propagande ou de désinformation, en accomplissant des humiliations symboliques, ce qui, cette fois suppose de faire circuler des messages trompeurs, provocateurs ou hostiles contre le gré de cet État et en dépit de systèmes de sécurité. Ainsi la "défiguration" du site de l'ambassade de France en Chine au moment des manifestations pro-tibétaines.

Par ailleurs, nous avons également souvent signalé la difficulté de distinguer un "acte" de cyberguerre du cybercrime en général, forme de délinquance qui existe, elle, sans aucune contestation, voire du "cyberterrorisme", qui consisterait à saboter à distance les systèmes informationnels d'un pays ou d'une institution dans un but politique. Dans ce dernier cas, la difficulté est de savoir si l'attentat, ou son équivalent numérique, émane de groupes privés militants ou de services d'État (et plus vraisemblablement de services secrets manipulant des groupes "privés" de pirates informatiques).

Mais cela n'épuise pas la question.

Quand bien même on parlerait de *lutte à travers le cyberespace*, sans employer le mot tabou de guerre, resterait cette nouveauté incontestable : une entreprise menaçant un État qu'elle accuse plus ou moins d'espionnage de se retirer de son territoire et de le priver de sa technologie. Pendant que l'État qui serait censé se tenir du côté "victime", à savoir les USA, se contente très classiquement de demander des "explications" par les voie diplomatiques.

Que s'est il passé, en effet ?

Version la plus courante : en dépit des 384 millions d'internautes chinois, Google pourrait se retirer du pays en riposte à la "grave atteinte" à la propriété intellectuelle qu'a subi cette compagnie vers la mi-décembre. Les attaques venues de Chine , attaque éventuellement relayée par des complicités humaines au sein de Google, auraient procédé en deux vagues. La première qualifiée d'ultra-sophistiquée s'en serait prise à des codes sources de logiciels Google. La seconde, travaillant de façon plus rustique par "phishing" (attaque qui consiste à "hameçonner" une victime en se faisant passer pour un site officiel comme un banque pour l'amener à vous donner des informations confidentielles). Les victimes auraient été des militants chinois des droits de l'homme. Des "douzaines de comptes" précisait même le responsable juridique de la firme.
Conclusion logique : un pays totalitaire se livre à des manœuvres à grande échelle et persécute des démocrates et Google dont la devise est "be no evil" (ça ne s'invente pas !) réagit en lieu et place de l'État US, freiné par les usages diplomatiques.
Suivant une récente information, les attaquants seraient "passés" pour attaquer Google, par une faille de sécurité dans les versions 6,7 et 8 du célèbre navigateur Explorer. Du coup, les autorités allemandes et françaises (voir le communiqué du Certa) mettent en garde contre cette vulnérabilité. Bel exemple des nouvelles interactions entre politique et technologique !

À y regarder de plus près, cependant, les choses sont un peu plus complexes :
- L'attitude de Google, d'abord. La société avait passé un accord avec le gouvernement chinois en 2006 pour censurer son moteur de recherche version chinoise (google.cn) Ainsi, sur son portail, quelqu'un qui tapait "place Tien An Men" ne pouvait trouver que des photos officielles et rien qui rapporte les révoltes de 1989. Inutile de dire que l'affaire a fait plutôt mauvais effet et que Google avait à se faire pardonner.

Par ailleurs, les mauvaises langues suggèrent que, si le marché chinois est immense, sa rentabilité financière de quelques centaines de millions de dollars seulement n'est pas si fabuleuse à l'échelle de Google. La compagnie de Larry Page and Sergey Brin s'était déjà accrochée plusieurs fois avec les autorités chinoises dont les demandes augmentait ; elle semble même avoir déjà envisagé de quitter la Chine, marché peu rentable et dangereux en termes d'images de marque. La décision pourrait être la suite d'une stratégie réfléchie et non pas une réaction indignée face aux persécutions d'opposants.

Quoi qu'il en soit, le fait que Google se conduise comme une puissance souveraine et sanctionne un État, menant ainsi sa véritable politique étrangère, traduit bien une réalité de la mondialisation : l'émergence des grands acteurs économiques dans le domaine géopolitique, leur capacité de se présenter comme les véritables acteurs de l'histoire, en lieu et place des appareils étatiques dépassés. Voire de les "punir".

- La finalité des deux vagues d'attaque (la "sophistiquée" et la seconde) n'est pas si claire. D'autant que la première vague n'aurait pas touché que le fameux moteur de recherche, mais une vingtaine de sociétés US (voire 35 selon d'autres sources). Tout cela pour se procurer l'adresse ou la correspondance de pro-tibétains ? Difficile à croire. Attaquer Adobe, Northrop Grumman et Dow Chemical, pour prendre quelques noms cités, ne semble pas une façon très logique de persécuter les amis du dalai-lama ou des droits de l'homme. Il semble beaucoup plus logique de penser qu'il s'agit d'espionnage informatique de haut niveau, à but économique et s'en prenant également à des entreprises européennes.
Quant à la seconde vague d'attaques, si elle a touché, selon Google, "des dizaines de comptes mails" d'opposants sur gmail (les adresses électroniques fournies par Google), y compris en Europe, elle pourrait bien ne guère avoir de rapport avec la première. De là à penser qu'il y a, sinon amalgame, délibéré, du moins exploitation médiatique pour mettre sous l'étiquette "défense des droits de l'homme" des réalités qui relèvent plutôt de l'espionnage industriel...

- La culpabilité chinoise, ou plutôt celle du gouvernement chinois, est-elle si évidente ? Sur le plan formel, nous n'en avons aucune preuve. Certes, toujours selon Google, les comptes, tel celui de l'étudiante à Stanford d'origine tibétaine Tenzin Seldon, ont été piratés "depuis la Chine". Mais "depuis la Chine" (traduisez : que l'on à pu remonter jusqu'à une adresse IP se terminant en "cn") ne veut pas dire par les autorités chinoises. Cela signifie que l'attaque est passée par un ordinateur (peut-être infecté et manipulé depuis l'autre bout du monde) situé sur le territoire chinois.

Il y a deux autres hypothèses.

1°) qu'il s'agisse de "faux drapeaux" : des pirates non chinois pourraient parfaitement prendre à distance les commandes d'ordinateurs de ce pays. Des gens qui sont par définition capables de diriger des milliers d'ordinateurs zombies pourraient être assez intelligents pour penser à laisser de fausses pistes
2°) que les attaques partent bien du territoire chinois, mais qu'elles sont issues de groupes de hackers"patriotes", motivés politiquement, mais pas forcément par l'armée chinoise ou ses services.

Bien entendu, il ne s'agit pas d'être naïfs. Il existe des arguments contre la Chine :
- il est difficile de croire que dans un pays aussi surveillé, des "privés" puissent se livrer à ce type d'activités sans que l'État les connaisse, les contrôle, voire les manipule.
- des chercheurs, notamment des Canadiens de l'Université de Munk, pointent depuis mars dernier vers un réseau du nom de Ghostnet, une vaste structure d'espionnage électronique située sur le territoire chinois et qui aurait compris des ordinateurs de services officiels dans 103 pays
- la Chine, souvent désignée par les États-Unis comme responsable de multiples attaques contres les systèmes informationnels, tandis que les think tanks de Washington soulignent que ce pays se dote de capacité "cyberguerrières" en accord avec sa doctrine militaire.

Bref, nous nous trouvons confrontés aux questions récurrentes liées aux cyberattaques :
- celle de l'identification de l'agresseur, mais aussi de la nature de l'agression : à but intéressé (handicaper un concurrent, lui voler ses secrets), politique (exercer une contrainte sur un acteur souverain) ou idéologique et symbolique (défendre et illustrer une cause, en stigmatiser une autre) ?

- celle du "lieu" de l'attaque. Il y a ici contradiction entre la logique classique (une agression part de quelque part et frappe quelque part...) et celle du cyberespace (les attaques ne passent pas clairement par des zones relevant de la responsabilité d'un acteur souverain comme une troupe d'hommes en armes passerait par un territoire où un État est censé exercer son monopole de la violence légitime).

En d'autres termes, il s'agit d'un question de frontières à la fois au sens distinguo entre des catégories (privé/public, politique/économique, militaire/civil), mais aussi au sens topologique, une ligne projetée sur la carte : si la frontière politique détermine deux zones d'exclusivité (ici j'exerce ma justice, j'utilise ma monnaie, j'exerce mon droit, je possède mes armées, j'accueille et interdis, là est ton territoire...), le savoir, le pouvoir et la violence circulent sur Internet suivant leur propre logique que nous tenterons de développer dans un prochain article.

8 septembre 2007

Rififi dans le cyber village : des sources officielles américaines accusent une nouvelle attaquer les réseaux informatiques de la défense américaine. De quoi relancer l'idée d'une cyberguerre par écrans interposés qui pourrait maintenant toucher la France.. Suivant le Financial Times, l'armée populaire de libération chinoise s'est livrée depuis des années à des centaines de cyberattaques contre les réseaux du Pentagone. En Juin dernier, elle aurait réussi à pénétrer jusque dans le bureau de Robert Gates, le Secrétaire américain à la Défense.
Cette affaire fait suite à une autre où les militaires chinois auraient tenté d'introduire des « chevaux de Troie » dans les ordinateurs du gouvernement allemand ce qui aurait fait l'objet d'un incident entre Angela Merkel et le premier ministre chinois Wen Jiabao. Avec un pareil dossier, il y a de quoi faire des gros titres, et surtout il y a de quoi raviver une vieille inquiétude de la Défense américaine exprimée depuis les années 90 : qu'un Etat voyou formant ses propres spécialistes ou engageant des pirates informatiques n'utilise la toile pour mener des offensives contre les réseaux informatiques dont dépend la sécurité nationale.
Personne ne prétend que l'armée chinoise soit composée de naïfs ou d'enfants de chœur. Il est donc tout à fait vraisemblable que comme toutes les armées du monde, à commencer par celle des Etats Unis, elle s'est dotée de moyens d'attaque et de défense via les réseaux informatiques. Qui plus est, la doctrine militaire chinoise, ou du moins ce que nous en savons à travers le livre La guerre hors limite (traduit chez Payot), préconise justement ce type d'opérations. Dans une logique héritée de la tradition stratégique de Sun zi et Sun bi, l'armée chinoise recherche l'économie de moyens, surtout par rapport à un adversaire technologiquement suréquipé. Cette force de l'adversaire éventuel, il faut la transformer en faiblesse. C'est pourquoi, la guerre chinoise de demain sera aussi une guerre de l'information, une guerre économique, une guerre électronique, etc.…
Pour résumer : les Chinois ont l'intelligence, la capacité, et la motivation pour le faire. Est-ce la preuve qu'ils l'ont fait ? D'une part, comment prouver que les attaques contre le Pentagone aient été menées par la Chine ? Quand bien même on pourrait les retracer jusqu'à des ordinateurs sur le territoire chinois, la démonstration laisserait place au doute. D'autre part, si l'on examine d'un peu plus près la nature des terribles cyberattaques, on s'aperçoit qu'il s'agit d'une pénétration dans un réseau de courriels non protégés réservés aux conseillers politiques du Ministre de la Défense. Dans le cas de l'Allemagne également, les logiciels malicieux que l'on suppose introduits par l'armée chinoise, devaient servir à prélever de l'information, nullement à détruire des mémoires ou des circuits de commandement. Au fond, si l'on peut parler de cyberespionnage, il n'y a là rien qui ressemble à une agression militaire. Une fois de plus, le terme de cyberguerre semble être utilisé comme un constat attrappe- tout, sexy et sans consistance (après tout, pour qu'il y est guerre, il faut au minimum qu'il y ait mort d'hommes et continuité d'une violence organisée).
En revanche, la révélation de ce danger chinois, tombe à pic quelques mois après les accusations lancées contre la Russie qui aurait mené sa propre cyberguerrre contre l'Estonie (en réalité : un déni de service qui avait paralysé des serveurs estoniens pendant quelques heures). L'armée américaine semble une vivante illustration de l'adage « Tout est clou pour celui qui a un marteau » : elle continue à projeter sur ses adversaires sa propre logique, celle d'une guerre high tech dans la continuité de la "Revolution in Military Affairs"

L'affaire n'est pas neuve. Les « ennemis d'Internet », entendez les gouvernements autoritaires, se sont toujours efforcés de contrôler la Toile, ou, du moins, d'empêcher leurs

citoyens de recevoir des contenus subversifs de l'extérieur, de laisser filtrer de l'information gênante hors de leurs frontières et de créer des espaces numériques de discussion critique. Jusqu'à présent les experts pensaient que le parti de la censure perdrait forcément à long terme.
Ils s'appuyaient sur plusieurs postulats qui se sont tous révélés faux :
- Internet était intrinsèquement porteur de liberté. Le développement des réseaux impliquait à la fois un accès potentiellement illimité à un information pluraliste et des possibilités de s'exprimer si vastes qu'elles seraient vite incontrôlables. La technique répandrait la liberté et seuls quelques esprits archaïques chercheraient vainement à freiner cette évolution inéluctable.
- Du reste développement des technologies de l'information et de la communication, développement économique par le libre jeu du marché et développement politique (entendez instauration d'une démocratie à l'occidentale) allaient de pair. Ce sens de l'histoire avait même un nom : c'était l'élargissement (enlargment), suivant le modèle global de la société de l'information. Ainsi, combler le fossé numérique contribuerait à répandre prospérité, esprit critique et valeurs démocratiques.
- Les États qui tenteraient de s'opposer au libre flux de la communication y parviendraient de moins en moins au fur et à mesure que leurs citoyens seraient mieux connectés, plus conscients et plus prospères. Face à cette résistance d'arrière-garde, l'esprit libertaire des internautes trouverait cent moyens nouveaux de ridiculiser les gendarmes de la Toile. Vouloir défendre un quelconque monopole de la pensée à l'intérieur de frontières nationales était une absurdité évidente à l'époque de la mondialisation et du village global. Que nous enseigne l'exemple chinois ?
- Un État moderne peut concilier des taux de développement économique spectaculaires et une idéologie communiste. Il peut adopter les règles du marché, s'équiper de moyens modernes (avec plus de cent millions d'Internautes, la Chine est le second marché du monde après les USA) et ne pas changer son système politique.
Or celui-ci repose en grande partie sur la domination des moyens de faire savoir et de faire croire
- L'État peut techniquement contrôler les flux d'information sur son territoire. Internet, contrairement à une idée reçue n'est pas un espace sans frontière. Bien sûr ce contrôle
– comme tout contrôle de frontières – est loin d'être parfait. L'internaute astucieux peut contourner les obstacles, utiliser des sites dits « anonymiseurrs », ne pas se faire repérer par les autorités lors de ses navigations ou en utilisant certains termes interdits que repèrent les robots sémantiques...
Mais la majorité des internautes chinois reste soumise à deux contraintes. Une contrainte policière : surveillance des cybercafés, obligation de faire connaître son identité pour toutes sortes d'opérations, traces laissées par les connexions…
Une contrainte technique : pour aller sur Internet de Chine, il faut passer par un fournisseur d'accès sur le territoire chinois qui peut contrôler votre identité, vos connexions, les termes que vous employez dans vos mails ou sur votre blog et qui peut vous refuser l'accès à des sites interdits. Ainsi, un serveur de messagerie qui est situé sur le territoire de la Chine est soumis à la fois à sa législation et à sa surveillance des contenus. Or toutes nos connexions et transactions sur Internet laisse une trace numérique.

Si vous ne savez pas où aller chercher des images ou des textes interdits, vous ne risquez guère d'être atteint par eux. Le tout sur fond de contrôle linguistique : sa langue a toujours été une des meilleures défenses de la Chine contre les influences du monde extérieur.

Problème : comment empêcher un chinois d'aller chercher des contenus subversifs sur un moteur de recherche en chinois hors de Chine ? Réponse : en créant votre propre moteur de recherche sur le territoire national (Baidu) et en passant des accords avec Yahoo, Google ou Msn, alléchés par un gigantesque marché. Ainsi, les capitalistes yankees, si enclins à tenir un discours moderniste et libertaire ou à invoquer les droits de l'homme, se feront un plaisir de créer des moteurs de recherche locaux « bridés » suivant les demandes des autorités. , de « limiter » ces moteurs sémantiques et les portails, de fournir des techniques de surveillance, de traçage et de blocage d'accès, comme les milliers de «routeurs» de Cisco vendus à la Chine et qui repèrent les mots interdits. Ils pourront même transmettre les éléments pour inculper un dissident.
Résultat : d'après Reporters Sans Frontières, il y aurait 49 cyberdissidents emprisonnés en Chine : un chiffre minuscule à l'échelle du pays, mais un signal fort. Cerise sur le gâteau : les autorités de Pékin par la voix d'un responsable du Bureau d'Etat de l'Information, Liu Zhengrong peuvent se permettre de répondre aux Occidentaux : mais nous ne faisons que la même chose que vous ! Vous luttez contre les sites révisionnistes, terroristes ou pédophiles, nous protégeons nos citoyens contre la pornographie et la subversion.
Le sous-comité des relations internationales de la Chambre des Représentants a violemment pris à partie les sociétés US concernées à commencer par Yahoo (dont on dit qu'il aurait donné des informations permettant d'inculper deux de ses abonnés chinois) et Google (qui avait pourtant longtemps résisté à la pression de Pékin et avait même était « fermé » quelque temps en chine). Mais celles-ci répondent que c'est après tout au gouvernement US de régler le problème sur le plan diplomatique. Le pouvoir politique qui a adopté le Global Internet Freedom Act est-il désarmé face aux activités des entreprises privées hors de ses frontières ? Ce n'est pas certain. La législation sur l'exportation des technologies sensibles permet d'exercer une pression.
Le Congrès pourrait imposer aux serveurs de messagerie de s'implanter hors des territoires d'États répressifs. Et il existe encore d'autres moyens. Ils ont d'autant plus de chance d'être explorés que l'offensive contre la censure sur Internet est menée simultanément par des représentants démocrates et républicains également hostiles à la « Realpolitik » de compromission commerciale avec des régimes suspects. Mais dans tous les cas, cette affaire nous aura rappelé une vérité : Internet est et reste un enjeu géopolitique. Que ce soit dans le domaine économique ou militaire, celui de la lutte contre le terrorisme ou celui de l'influence linguistique, idéologique et culturelle, c'est même un des domaines les plus disputés.