

30 mars 2010



## **LA CHINE ET GOOGLE** DECRYPTAGE D'UN CONFLIT

SOUS LA DIRECTION DE  
FRANÇOIS-BERNARD HUYGHE

*Chercheur associé à l'IRIS*



## " DEUX TIGRES NE PEUVENT PAS VIVRE SUR LA MÊME MONTAGNE " : L'AFFRONTEMENT DE DEUX MODÈLES

par Fabienne Clérot, chercheur associée à l'IRIS

L'affaire Google aura mis en évidence la compétition que se livrent les Etats-Unis et la Chine sur tous les terrains.

Depuis quelques mois, l'administration Obama semble avoir changé de stratégie à l'égard de Pékin en optant pour un discours de fermeté. Dans son discours du 21 janvier, la secrétaire d'Etat américaine Hillary Clinton a plaidé pour un internet sans frontières, a appelé les entreprises américaines à refuser la censure et n'a pas hésité à utiliser une terminologie digne de la guerre froide. " Un nouveau rideau est descendu sur l'information dans une grande partie du monde ".

La Chine a été clairement visée comme étant directement ou indirectement responsable des attaques informatiques récentes. Ces attaques auraient été lancées depuis 2 universités chinoises : l'université shanghaienne JiaoTong, célèbre pour son classement international des universités et la Lanxiang vocational School dans le Shandong.

Après avoir nié toute implication, le gouvernement chinois a montré un signe de sa bonne volonté en annonçant avoir fermé un important site d'entraînement au hacking (Black Hawk Safety Net), puis a répliqué en affirmant que la Chine, loin d'être coupable était au contraire la première victime des cyber attaques (surtout en provenance des Etats-Unis) et qu'elle entendait renforcer la coopération régionale et internationale en matière de lutte contre la cyber criminalité.

Selon Pékin, les Etats-Unis profitent d'internet pour exporter leur politique et leur culture. La Chine les accuse également d'utiliser les réseaux sociaux comme Twitter (bloqué en Chine) pour déstabiliser certains pays, notamment l'Iran. Plusieurs journaux chinois ont flatté la fibre nationaliste chinoise en taxant les américains d'impérialisme et même de colonialisme. Chine Nouvelle a accusé Google d'être un instrument politique des Etats-Unis, lié aux services de renseignements américains. Radio Chine internationale a vu dans l'affaire Google une attaque contre la souveraineté de la Chine. : "Seul dans les plus de 100 ans de colonialisme et de semi-colonialisme, il y a eu un tel exemple. C'était la Compagnie des Indes orientales britannique qui voulait contrôler la souveraineté de l'Inde". Global Times a accusé les Etats-Unis d'être " le premier pays à lancer la cyber-guerre ", avec " une armée de 80 000 personnes dotées de plus de 2 000 virus informatiques ".

Aujourd'hui, en Chine, Google semble bien isolé. Si sa bataille au nom de la liberté d'expression et contre la censure a eu un énorme impact médiatique, lui a valu le soutien d'une partie des internautes chinois et lui permettra peut-être de renforcer son image et ses parts de marché dans le reste du monde, les autres firmes américaines ne comptent pas suivre son exemple et entendent bien rester et se développer en Chine (Microsoft avec Bing, ou Yahoo géré par Alibaba). En outre, certains des partenaires chinois de Google, dans le domaine de l'internet mobile, lui ont déjà tourné le dos et on voit mal comment les entreprises publiques China Mobile et China Unicom pourraient continuer à proposer un moteur de recherches qui a défié les autorités.

Les autorités chinoises ont-elles essayé de retenir le géant américain ? Qui avait le plus à perdre dans ce départ ?

Il était illusoire de penser que Pékin puisse reculer sur la question de la censure, comme le demandait Google. Alors que les tensions sociales sont fortes et que la contestation et les mobilisations collectives se multiplient sur le web, Pékin est depuis plusieurs mois entré dans une phase de renforcement de son arsenal de contrôle afin de promouvoir ce qu'il nomme " un environnement online vert, sain et harmonieux ".

Le désengagement de Google renforce les leaders nationaux du web, au premier rang desquels Baidu [1] . En ces temps de "préférence nationale " voire de protectionnisme, ce n'est pas pour déplaire aux autorités chinoises.

La Chine se positionne rapidement et sûrement comme " l'autre pays du web ". Elle est d'ores et déjà le premier pays mondial en termes de démographie sur Internet et les taux de croissance sont impressionnants. La Chine entend-elle devenir le nouveau pays décideur sur Internet ?

D'anciennes déclarations de Jack Ma, le fondateur d'Alibaba, sont particulièrement éclairantes ! En octobre 2007, il prévenait déjà : "Nous avons acheté eBay, acheté Yahoo! et l'argent que nous avons sera utilisé pour stopper Google. Je les appelle les requins de l'océan. Nous, nous sommes des crocodiles dans le Yangtsé, nous avons donc plus de chance qu'eux.". Interrogé par l'agence Reuters sur ses relations avec Yahoo, il affirmait également: "Je fais les choses comme je l'entends. Je n'écoute pas Yahoo". "S'ils restent, très bien. S'ils partent, tant mieux. C'est ainsi que nous faisons des affaires."

La polémique aura peut-être l'effet inverse de celui qui était recherché par Google. Le principe de la censure n'a évidemment pas été remis en cause par le gouvernement chinois et le site hongkongais de Google est filtré en Chine continentale. Par ailleurs, Pékin a décidé de renforcer son contrôle sur les noms de domaine en .cn et entend mener un audit des domaines déjà déposés en réexaminant tous les dossiers et en n'excluant pas le cas échéant des fermetures [2].

Le gouvernement chinois semble plus que jamais capable de résoudre le dilemme que lui posait a priori internet, en en faisant à la fois un outil de modernisation économique et un instrument de contrôle politique. Mais de nombreux internautes chinois, entendent bien conserver l'espace de liberté ouvert par le net et rivalisent d'inventivité pour détourner la censure ou pour la ridiculiser. Ainsi l'harmonie (hexie), l'un des concepts politiques cher au Président Hu Jintao, est devenue sur le web chinois un synonyme de la censure, comme l'est par extension, du fait de son homophonie, l'expression " crabe de rivière " . " Etre harmonisé " ou " être encrabé " signifient en argot internet qu'une information a été supprimée ou bloquée par la censure.

La Chine construit progressivement son propre modèle de web, plus proche d'un vaste réseau intranet national dont les contenus seraient contrôlés et approuvés, tout en développant l'internet de demain [3] et en poussant ses groupes de médias à l'international pour jouer un rôle à la hauteur de sa nouvelle puissance et contribuer à son rayonnement. Comme dans les autres domaines, elle entend définir ses propres règles.

### **VERS UNE GUERRE DE L'INFORMATION ?**

L'opération Aurora, dont Google et d'autres sociétés ont été victimes, n'est ni la première ni la plus grave attaque informatique. Alors, pourquoi Google a-t-il décidé de rendre ces attaques informatiques publiques, pourquoi a-t-il fait appel à la NSA ? Pourquoi le gouvernement américain s'est-il emparé du sujet pour en faire une affaire politique ? Faut-il voir dans ce bras de fer une méthode de dissuasion à l'encontre de la Chine ?

Le cyberspace est devenu un champ de bataille dont les enjeux dépassent la sphère économique. Les Etats Unis s'inquiètent de plus en plus des questions de cyber sécurité comme le montre le dernier rapport de la US-China Economic and Security Review Commission [4], particulièrement alarmiste, ou la nomination par le Président Obama fin 2009 d'un responsable national de la sécurité sur Internet, chargé de coordonner la politique américaine dans ce domaine. La Chine consciente de la supériorité technologique des Etats-Unis sur le plan militaire, depuis la guerre du Golfe, mise beaucoup sur la guerre de l'information qui joue un rôle décisif dans la modernisation de son armée. La cyberguerre est du point de vue chinois une forme de guerre asymétrique rentable, parce qu'elle peut infliger des dommages considérables pour un coût minimal [5] .

La stratégie de guerre de l'information en Chine emprunte beaucoup aux traités classiques sur la guerre qu'il s'agisse des *36 stratagèmes* ou de *L'art de la guerre* de Sun Zi .

Par plusieurs de ses aspects (espionnage, adaptation aux circonstances, analyse des faiblesses de l'ennemi, ruse, dimension psychologique...), le concept chinois de guerre de l'information réinterprète les préceptes anciens : " Toute guerre est fondée sur la tromperie. ", " Qui connaît son ennemi comme il se connaît, en cent combats ne sera point défait ", " tout l'art de la guerre est basé sur la duperie ", " arrivez comme le vent et partez comme l'éclair ", " traverser la mer sans que le ciel le sache ", " assassiner avec une épée d'emprunt ", " bruit à l'est ; attaque à l'ouest ", " dissimuler une épée dans un sourire ", " attirer le tigre hors de la montagne " ...

La Chine se présente comme une nation pacifique [6] malgré la forte croissance des budgets de la défense. Le pays se dit uniquement préoccupé par la préservation de sa souveraineté et la défense de son intégrité territoriale [7] .

Certaines des attaques informatiques des dix dernières années visaient à défendre ce que Pékin considère comme ses intérêts nationaux : attaques contre des sites américains suite au bombardement de l'Ambassade chinoise de Belgrade



en 1999, contre des sites japonais en 2005, ou contre le Dalai Lama. Plus récemment, ce sont des administrations (ambassades) ou des entreprises qui ont été ciblées (opération Aurore). Outre la formation de militaires spécialisés dans ce domaine, la Chine compte aussi sur les "civils" (pirates isolés, hackers patriotes, instituts de recherche...) pour amplifier ses forces.

Afin d'être invulnérable aux attaques informatiques étrangères, la Chine aurait parallèlement développé son propre système d'exploitation sécurisé, appelé Kylin. Son développement aurait débuté en 2001, à l'Université nationale de la technologie de défense de Changsha.

L'affaire Google est-elle l'une des premières escarmouches dans la guerre de l'information entre les deux puissances ? Quelles en seront les conséquences ? Faut-il s'attendre à une escalade ? La guerre de l'information ne fait que commencer... ■

[1] Baidu a récemment entrepris de concurrencer Youtube (filiale de Google) avec Qi Yi en levant 50 millions de \$.

[2] Face à ces nouvelles mesures, GoDaddy, le plus grand registraire du monde a annoncé l'arrêt de ses activités en lien avec le domaine.cn.

[3] Standard IPv6

[4] Report on the Capability of the People's Republic of China to Conduct Cyber Warfare and Computer

[5] "Soumettre l'ennemi par la force n'est pas le summum de l'art de la guerre, le summum de cet art est de soumettre l'ennemi sans verser une seule goutte de sang." Sun Zi

[6] "Le gouvernement et le peuple chinois sont prêts à coopérer avec la communauté internationale afin de surmonter les obstacles, partager les opportunités de développement et apporter de nouvelles contributions à la paix et au développement dans le monde" Wen Jiabao, session ANP 5 mars 2010

[7] Question cruciale de Taïwan

# GUERRE DE L'INFORMATION ET CYBERGUERRE EN CHINE

par Daniel Ventre, ingénieur au CNRS

Plus un mois ne passe désormais sans que la Chine ne soit montrée du doigt, accusée d'être à l'origine de " cyber-attaques " touchant entreprises, administrations, infrastructures critiques aux Etats-Unis, en Europe, en Inde, en Australie, partout dans le monde. Intrusions dans les systèmes, vols de données, interceptions, propagation de malwares, attaques par botnets, défigurations de sites, exploitation de failles, les méthodes utilisées sont a priori celles de la cybercriminalité. Mais l'appât du gain financier n'est sans doute pas le seul motif. Les opérations peuvent servir d'autres intérêts: perturbation, destruction, renseignement, objectifs politiques, économiques, idéologiques, militaires. L'état de la technique ne permettant pas aujourd'hui d'attribuer les " attaques " de manière certaine, il est difficile d'affirmer l'implication de l'Etat chinois dans toutes les affaires qui lui sont attribuées.

La Chine n'en est pas moins devenue sur la scène internationale un acteur incontournable de la guerre de l'information (GI) et de la cyberguerre, ne serait-ce que pour avoir clairement affiché depuis près de 20 ans ses théories, doctrines, politiques ou stratégies en matière d'utilisation à des fins agressives et défensives du cyberspace. Cette approche chinoise de la GI et de la cyberguerre a deux facettes, militaire et civile, développées sur un plan à la fois théorique et pratique.

## LA DIMENSION MILITAIRE

Le succès fulgurant des Américains lors de la première guerre du Golfe fut interprété dans un certain nombre d'états-majors comme la victoire des nouvelles technologies. La maîtrise de l'information et des technologies de l'information conférait la maîtrise du champ de bataille. Cette conclusion appelait une transformation radicale au sein des forces armées. Le concept de GI s'est imposé à la Chine dans ce contexte. Depuis lors les militaires en ont assuré le développement et la mise en œuvre au travers de leur RMA guidée par le concept d'" *informationization* ". Une littérature riche a permis depuis le milieu des années 1990 de définir le concept de GI chinoise.

En 1995 le général Wang Pufeng, père de la doctrine chinoise de GI, la définissait comme une guerre dont l'objectif n'est plus la conquête de territoires ou la destruction des troupes adverses, mais la destruction de la volonté de résistance adverse. Une guerre dans laquelle la capacité à voir et à savoir avant l'adversaire, à agir plus vite, à frapper de manière plus précise est tout aussi importante que la puissance de feu

En 1997 le colonel Wang Baocun ajoutait que la GI peut être menée en temps de paix, de crise et de guerre ; consiste en opérations offensives et défensives ; a pour composantes principales les C2 (commandement et contrôle), l'intelligence, la guerre électronique, psychologique, la guerre de hackers, la guerre économique.

En 1999, les colonels Qiao Liang et Wang Xiangsui dans leur célèbre ouvrage " *La guerre hors limites - l'art de la guerre asymétrique entre terrorisme XE "terrorisme" et globalisation* ", soulignaient que " le progrès technique [...] a offert de nombreuses possibilités nouvelles de vaincre. Et tout cela nous permet de penser que le meilleur moyen de remporter la victoire, c'est de contrôler et non de tuer ". Cette forme de guerre moderne, les auteurs l'appellent " *guerre hors limites* " pour signifier que les armes, les techniques sont multiples, que " le champ de bataille sera partout ", qu'il n'y aura plus de frontière entre guerre et non guerre. " *Le champ de bataille est à notre porte et l'ennemi est en ligne* ", " *c'est la guerre permanente* ". La guerre de l'information est la " *guerre où l'informatique est utilisée pour obtenir ou détruire des renseignements* ".

Citons enfin la revue " *Liberation Army Daily* " qui en 2006 définissait la guerre de l'information en ces termes : " le mécanisme pour prendre le dessus sur l'ennemi dans une guerre sous conditions d'informatisation, trouve sa plus forte expression dans notre capacité ou non à utiliser plusieurs moyens permettant d'obtenir et assurer la circulation efficace de l'information ; notre capacité ou non à faire pleinement usage de la perméabilité, de la propriété de partage et de la connexion de l'information pour réaliser la fusion organique des matériels, de l'énergie, et de l'information, afin de créer une force de combat combinée : et dans notre capacité ou non à utiliser des moyens efficaces pour affaiblir la supériorité de l'information de l'ennemi et l'efficacité opérationnelle de l'équipement informatique ennemi".

Forte de ces approches théoriques, la modernisation de l'armée chinoise vise " l'informationization ", concept qui consiste à développer une architecture en réseau, permettant de coordonner les opérations militaires dans toutes les dimensions. La stratégie de guerre de l'information chinoise est condensée dans le concept INEW (*Integrated Network Electronic Warfare*), défini par le général Dai Qingmin dès le début des années 2000. L'INEW est l'intégration de la guerre électronique (EW) et des attaques par réseaux d'ordinateurs (CNA - *Computer Networks Attacks*) pour la partie offensive, et pour la partie défensive de la protection des réseaux (CND - *Computer Networks Defence*) et des opérations de renseignement (CNE - *Computer Networks Exploitation*). L'action conjointe de CNA et EW contre les C4ISR et les réseaux des systèmes logistiques adverses constitue la base de la guerre de l'information offensive chinoise.

En 2003, le Comité Central du Parti Communiste chinois a validé le concept des " 3 guerres ", concept de GI militaire dont les composantes sont la guerre psychologique, la guerre des médias (influencer l'opinion publique nationale et internationale), et la guerre juridique (qui consiste à recourir aux outils du droit national et international pour obtenir le soutien de la communauté internationale).

De nombreux centres de formation des armées (Zhengzhou, Wuhan, Changsha...) dispensent aux militaires depuis le milieu des années 1990 des enseignements en GI, et depuis 1997, la presse a fait état de nombreux exercices de GI menés par les forces armées, preuve du passage de la théorie à la pratique.

Les capacités réelles de la Chine en matière de GI et de cyberguerre demeurent une inconnue.

Quelles que soient ces capacités, constatons que la place prise aujourd'hui en Chine par la maîtrise de la dimension cybernétique au sein des armées est considérable puisque le niveau de développement de ces dernières se mesure à l'aune de celui des capacités de GI. Objectif poursuivi : être capable de gagner des guerres conduites par l'information (guerre de l'information, cyberguerre) d'ici à la moitié du 21<sup>e</sup> siècle.

La Chine est engagée sans ambiguïtés dans cette voie : " la cyberguerre n'est plus depuis longtemps affaire de science fiction", déclarait le colonel Dai Qingmin en 2009, ajoutant que " l'Internet deviendra le lieu d'une inévitable course aux armements".

## LA DIMENSION CIVILE

En 1995 le général Wang Pufeng 1995 évoquait la renaissance du concept de " guerre du peuple ", rendue possible par l'intégration des spécialistes civils et militaires dans une même lutte, le champ de bataille traditionnel n'existant plus, la guerre pouvant être partout, devenant l'affaire de tous.

Concrètement l'implication du secteur civil se traduit de diverses manières :

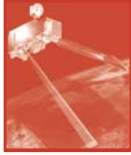
l'armée chinoise développe ses capacités en relation étroite avec l'industrie du secteur privé et le monde académique, mettant en pratique le rapprochement entre secteur privé et public, secteur civil et militaire, que l'on observe également dans nombre de nations industrialisées.

A la frontière du civil et du militaire, des unités de milice établies par l'armée dans les diverses provinces militaires, font appel à des citoyens travaillant dans l'industrie ou le monde académique. Ont ainsi été mises en place des unités ayant compétences dans la GI, la guerre électronique, la guerre psychologique, les opérations d'information, la guerre en réseau, etc.

Certaines sources évoquent les liens qu'entretiendraient certains fournisseurs de l'armée chinoise avec la communauté des hackers. On ne peut toutefois affirmer que l'armée chinoise ait la main mise sur cette communauté.

L'" *Annual Report on the Military Power of the People's Republic of China*", rappelait en 2003 les dangers propres au piratage nationaliste (hacktivisme) en période de tension ou de crise. De nombreuses actions sont à leur actif : vagues de cyberattaques consécutives au bombardement de l'Ambassade de Chine par les forces de l'OTAN à Belgrade en 1999 ; attaques contre les intérêts taiwanais ; attaques en règle contre les sites officiels américains en protestation à la collision entre un avion de chasse chinois et un avion espion américain en 2001 ; attaques contre les sites officiels tibétains ; en 2008, attaques contre le site internet de l'Ambassade de France en Chine suite à la rencontre entre le Dalai Lama et le chef de l'Etat français. La liste est longue.

La GI chinoise essentiellement vouée à gérer des rapports de force avec l'extérieur (assurer la place de la Chine sur la



scène internationale), s'applique également à l'intérieur du cadre de ses frontières : la maîtrise de l'information et de l'espace informationnel est affaire de pouvoir au sein même de la Chine.

Or les évolutions technologiques de ces dernières années jouent les trouble-fêtes. Les réseaux sociaux (Twitter, Facebook...) se sont invités sur la scène politique nationale. En août 2009 un article du site Ceneews (*Central European News in Chinese*) les qualifiait de nouvelle arme, d'outil de subversion, d'infiltration politique et culturelle d'un pays, d'outil de propagation de rumeur, d'outil politique puissant, d'outil de déstabilisation.

Le cyberspace est un système d'armes vulnérable. La Chine sait en jouer. Elle en subit aussi les contraintes. ■

*Daniel Ventre est ingénieur au CNRS. Il enseigne à Telecom ParisTech, à l'ESSEC Business School Paris. Il a publié, en 2009, un ouvrage intitulé « Information Warfare ».*

## GOOGLE IS GO(O)D

par Stéphane Charrière, co-fondateur de l'Observatoire Alterbrand\*

**Au commencement était le Verbe.** Et le Verbe était avec Google. Et le Verbe était *to google*.

Dès 2003, soit à peine cinq ans après la naissance de Google, le néologisme faisait son entrée dans l'Oxford Dictionnaire. En 2007, le nombre de clients de la régie publicitaire de Google dépassait le million. En 2008, le nombre de pages indexées par le moteur de recherche Google dépassait le trillion. En 2009, plus de 777 millions de fidèles se tournent quotidiennement vers Google, qui exauce chaque jour 3 milliards de requêtes en 45 langues[1].

Au commencement, donc, était le Verbe. Et le Verbe était un agent double.

D'un côté, les mots-clés que nous confions à Google nous donnent accès à toute l'information du monde. De l'autre, simultanément, ces mêmes mots-clés renseignent Google sur ce qui nous intéresse, et qui, par là-même, nous qualifie pour un lien publicitaire aussi opportun, précis, pertinent que possible.

Ainsi Google échange des informations contre des mots (grâce à son moteur de recherche), et des mots contre des dollars, ou toute autre devise en vigueur (grâce à sa régie publicitaire qui diffuse des annonces ciblées.) Toute l'information du monde contre toute la psyché du monde.

La dualité du Verbe - la capacité des mots-clés à renseigner conjointement un utilisateur et un annonceur - fait dès lors de Google une machine économique inédite.

Son potentiel de conquête ? Aussi vaste que l'économie : toute entreprise souhaitant être trouvée sur Internet. Sa matière première ? Gratuite, inépuisable, hautement malléable : toutes les combinaisons de mots, de tous les mots, dans toutes les langues. Son outil de production ? Vertueux à plus d'un titre.

Vertueux, parce que le rythme des requêtes ne cesse de croître, et que chaque nouvelle requête fournit à Google l'opportunité d'afficher des liens commerciaux ciblés.

Vertueux, parce que chaque clic sur ces liens est vendu aux enchères, auprès d'une communauté d'annonceurs Google également en forte croissance.

Vertueux, surtout, parce que Google a fait de la vertu l'axe fondamental de sa compétitivité.

" *Don't be evil*." Le prophète Jobs, qui représente un culte aujourd'hui concurrent, est revenu récemment sur le premier commandement de Google, sur un ton à la limite de l'evil : " *Their 'don't be evil' mantra : it's bullshit*." [2]

*Bullshit*, bien sûr, si l'on y voit tout juste l'expression bon enfant d'une éthique d'entreprise, calquée sur les valeurs de son milieu d'origine.

*Bullshit*, d'autant plus, lorsque le président de Google formula, à propos de la censure chinoise des résultats de recherche, la doctrine toute jésuitique d'une " *échelle du mal* " [3].

Pour autant, une interprétation purement morale de ce *'don't be evil'* est une fausse route.

*Don't be evil* résume en premier lieu un principe fondateur du moteur de recherche : la pureté des résultats naturels, vierges de toute influence commerciale qui viendrait à fausser leur qualité et tromper ses utilisateurs.

Un principe de séparation de l'Eglise et de l'Etat - l'information d'un côté, le commerce de l'autre - dont la finalité est avant tout économique : traitons nos utilisateurs du mieux possible, et le profit suivra, même et surtout si les marchands restent à la porte du Temple.

Dès lors, plutôt qu'un impératif moral, *don't be evil* définit d'abord l'axe central de la supériorité de Google : *others are evil, think different*. La référence au mal y est avant tout l'expression d'une stratégie de rupture par rapport aux pratiques établies.

Un algorithme pur de toute influence commerciale est meilleur qu'un moteur qui mélange les genres. Une page d'accueil dédiée à la recherche, vierge de toute pollution (notamment publicitaire), est meilleure qu'un portail gorgé d'incitations, de sollicitations, de messages inutiles. Un lien publicitaire ciblé, opportun, que l'annonceur ne paye que lorsqu'il est cliqué, est meilleur que la déperdition propre aux mass media.

Ces parti-pris ont permis à Google de s'imposer, non seulement face aux moteurs de recherche concurrents, mais aussi plus largement

face aux portails internet, et surtout face aux régies publicitaires concurrentes. Une rupture sur le marché de la publicité, ou plutôt contre la publicité traditionnelle : contre la déperdition qui affecte son *Return On Investment* (côté annonceurs), contre la pollution qu'elle représente parce qu'elle est envahissante, bavarde, inopportune (côté utilisateurs). Une rupture source de profit : *one can earn money without being evil* - qu'il serait plus exact de traduire par : *not being evil is a better way to earn money*.

Google est ainsi une formidable machine morale ; non pas une machine au service d'une morale pré-existante, mais bien plutôt une machine qui écrit, à son avantage, sa propre morale des affaires, et s'en sert pour créer et conquérir des marchés[4].

C'est selon ce même prisme économique et pragmatique qu'il faut relire les récentes déclarations d'Eric Schmidt sur les questions de confidentialité.

" *If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.*" [5] *Don't be evil*, version longue ?

Google, œil de Cain ? Les commentateurs furent unanimement surpris qu'une entreprise comme Google, qui revendiquait jusqu'alors le respect de ses utilisateurs comme valeur cardinale, se permit pour l'occasion de les juger, voire de les menacer.

Pourtant, par-delà Bien et Mal, le propos d'Eric Schmidt doit se lire avant tout pour ce qu'il est : une défense inconditionnelle de la circulation de l'information, libre et sans entraves, gage de croissance actuelle et future.

C'est là la véritable " morale " de Google, celle que l'entreprise véhicule, et qui à son tour accompagne le développement de l'entreprise, et qui n'est écrite dans aucune charte, ni dans aucun rapport annuel.

" *Information wants to be free.*" [6] La formule fut lancée en l'an 14 avant Google. Quoiqu'elle n'ait jamais été reprise telle quelle par l'entreprise, elle semble en guider chaque développement, chaque prise de position. Sous des apparences innocemment libérales et technophiles, elle recèle un réel potentiel de subversion.

L'information veut être libre. Elle le veut doublement, par la volonté de ses utilisateurs, et par la diminution vertigineuse de son coût de diffusion. Cette volonté est aujourd'hui partout à l'œuvre. Elle affectait jusqu'à présent, modestement, des marchés entiers ; on la retrouve désormais au cœur des préoccupations des états.

L'information veut être libre en Chine. C'est-à-dire, pour l'essentiel, échapper à toute interférence étatique, qu'elle relève de la censure ou de la surveillance.

L'information veut être libre en Iran. Un pays qui a fêté à sa manière - par des attaques informatiques contre Gmail - les nouvelles fonctionnalités sociales du service de messagerie de Google, lancées imprudemment quelques heures avant l'anniversaire de la Révolution.

L'information veut être libre en Italie - elle s'y affronte à la volonté du gouvernement de rendre Youtube (la plateforme de partage vidéo de Google) responsable des atteintes portées par ses utilisateurs au copyright.

L'information veut être libre en France. Mais Google - " *aussi sympathique soit-il, aussi important soit-il, aussi américain soit-il*" [7] - y donnera bientôt son nom... à une taxe. Une contribution modeste aux recettes fiscales ; mais un hommage éclatant du pouvoir politique aux pouvoirs de Google, tant réels que symboliques.

*Nolens volens*, Google se révèle être bien plus qu'une machine économique : une machine idéologique radicale. C'est là son plus grand pouvoir : sa capacité à remettre profondément en question les pouvoirs établis - qu'ils soient culturels, économiques ou politiques. C'est également, à l'heure d'une coopération accrue avec les pouvoirs publics américains, son plus grand défi. ■

*\*Stéphane Charrière est co-fondateur de l'Observatoire Alterbrand (stephane@alterbrand.com).*

[1] Source : Comscore.

[2] " Leur devise, 'ne fais pas le mal' : *bullshit !* " - Steve Jobs, rapporté par Wired.com, 30/01/2010.

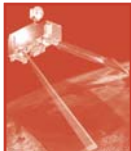
[3] " *We actually did an evil scale and decided not to serve at all was worse evil* " - Eric Schmidt, Davos, 2006, rapporté par le Wall Street Journal

[4] Alors que le marché mondial de la publicité a reculé de 12% en 2009, sous la barre des 425 milliards USD (source : PricewaterhouseCoopers), le chiffre d'affaires de Google a connu une croissance de 9% pour s'établir à 24 milliards USD en 2009.

[5] " S'il y a une chose que vous voulez faire sans que personne ne vous voie, peut-être devriez-vous tout simplement vous abstenir de faire cette chose. (...) Aux Etats-Unis, nous sommes tous soumis au Patriot Act, et il est possible que les autorités aient accès à cette information " / " *If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place* (...) *We're all subject, in the US, to the Patriot Act, and it is possible that that information could be made available to the authorities.*" - Eric Schmidt, CNBC, 12/2009.

[6] " *Information wants to be free. Information also wants to be expensive. Information wants to be free because it has become so cheap to distribute, copy, and recombine - too cheap to meter. It wants to be expensive because it can be immeasurably valuable to the recipient.*" - Stewart Brand lors de la première Hackers' Conference ; compte-rendu publié en 1985 dans Whole Earth Review.

[7] Discours de Nicolas Sarkozy à Geispolsheim - rapporté par Reuters - 10/12/2010



## GOOGLE DANS SON PLUS SIMPLE APPAREIL L'ENTREPRISE LA PLUS FORTE DU MONDE

**Interview de Olivier Jeandel, ingénieur spécialisé en développement de projets internet.  
Propos recueillis par Clément Petiet**

**OBSERVATOIRE GÉOSTRATÉGIQUE DE L'INFORMATION : Avec vous nous allons essayer de comprendre ce qu'est Google. Qu'est-ce que l'entreprise Google, aujourd'hui ?**

**OLIVIER JEANDEL :** Aujourd'hui, Google, c'est une des plus grosses multinationales au Monde. C'est une société basée à Mountain View, dans la *Silicon Valley*, créée seulement depuis 1998 par deux personnes : Larry Page et Sergey Brin. A la base, c'est juste un moteur de recherche pour devenir une société qui englobe 170 services : publicité en ligne ou gestion d'agenda, de comptabilité... Bien sûr le moteur de recherche reste le modèle phare. Aujourd'hui, 20.000 employés à travers le Monde entier. C'est le moteur de recherche incontournable.

**Comment expliquez-vous le succès de ce moteur de recherche ?**

Quand Google est arrivé en 1998, il existait déjà une petite dizaine de moteurs de recherche qui fonctionnaient très bien. Donc ils sont arrivés après les autres mais ils ont réussi à développer un algorithme de recherche et d'indexation des pages Web beaucoup plus précis et rapide que les autres. Petit à petit, ils ont réussi à indexer beaucoup plus de pages et à rendre ces sites plus accessibles aux internautes. La recherche était donc beaucoup plus pertinente via Google que via Yahoo ou Lycos. L'utilisateur retrouvait beaucoup plus facilement et rapidement ce qu'il recherchait. Le premier résultat correspondait à ce qu'il souhaitait contrairement aux autres moteurs de recherche.

**Aujourd'hui, s'ils on créé une page Web on la retrouve plus rapidement sur Google que sur les autres ?**

On la retrouve en 4 ou 5 jours. Tout se joue sur le référencement de cette page sur Google. Cela dépend de règles plus ou moins simples qui permettent d'affiner ce résultat. Google met à disposition des *Webmasters* (créateurs de sites) des outils qui permettent à leurs sites d'être mieux référencés.

**On crée notre site demain. Va-t-on sur Google pour avoir les outils qui peuvent nous aider ?**

Exactement. Comme Google Webmaster 2. Il fournit tout ce qu'il faut pour être bien référencé et est totalement gratuit.

**Tous les outils Google sont-ils gratuits ?**

La plupart le sont. Seuls quelques-uns sont payants. Dès lors que cela devient de la publicité, citée en tant que telle. Tout ce qui est Google Add Words. C'est du marketing annoncé sur le Net, de la publicité affirmée. Sinon, la plus part des services sont gratuits : Youtube, Picasa, Gmail ou Goggles Maps. 90% des produits.

**Google contrôle-t-il certains sites et refuse-t-il de les indexer ?**

La philosophie de Google, à la création, est de rendre l'information libre et gratuite à tous. Eux-mêmes s'obligent à ne pas censurer. Il ne font aucune censure sur ce que leur moteur de recherche indexe : sites pornographiques ou terroristes. N'importe qui peut y voir accès s'il fait les recherches adéquates.



### **Pour vous, informaticien, cela reste-t-il La référence ?**

Cela reste le modèle de l'entreprise rêvée. Elle se crée au bon moment, se développe très rapidement et a des produits de qualité. Aucune autre entreprise n'a réussi un tel développement en restant accessible. Pour tout faire : recherches, mails ou shopping, c'est le top. Dans ma société, le patron utilise Google tous les jours. C'est sa *road map*. Si Google devait fermer, nous serions bien embêtés.

### **Google passe-t-il en situation de monopole ?**

L'Internet évolue très rapidement. Aujourd'hui, c'est Google. Demain cela peut être une autre entreprise qui prend le dessus. Si elle n'allait plus très bien, quelqu'un reprendrait tout de suite le flambeau. Si Google est leader, il n'en reste pas moins perfectible. Pour exemple, Apple vient de signer un contrat avec Microsoft alors que le premier outil de recherche sur iPhone est Google. Les entreprises se battent sans cesse. Il y a, tous les jours, de nouveaux accords qui se font. Cela est loin d'être un monopole, comme on l'a reproché à Microsoft. Sur chaque produit, il y a un concurrent spécifique. :Yahoo pour Gmail ou Mappy pour Google Maps. Il existe toujours une alternative. Il n'existe pas de contrôle du Grand Manitou. Nullement comme Internet Explorer, autrefois, obligatoire lorsque l'on utilisait Windows.

### **Google fait-il des partenariats avec ses adversaires ?**

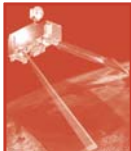
Non. C'est nettement la situation inverse qui se produit : les concurrents s'allient contre Google. Preuve en est le partenariat entre Yahoo et Microsoft, deux opposants à l'origine. Ils s'allient afin de détrôner Google AddWords, leader des solutions de publicités sur Internet. Google n'a pas besoin de partenaires. Il truste, petit à petit un maximum d'entreprises dans son spectre de développement. Il essaye de croître en externe.

### **En a-t-il les moyens ?**

Google, c'est 20 milliards de dollars de Chiffre d'Affaires annuel et 125 milliards de capitalisation en 2009. Aucune société ne rivalise, en terme de croissance, avec Google. Apple et Microsoft font très bien. Mais, en terme d'évolution, c'est le plus gros succès connu. ■

*Olivier Jeandel est un jeune ingénieur spécialisé en développement de projets internet. Il est diplômé de l'école Centrale Marseille en ingénierie mécanique et de l'ESSEC en management de projet.*





# DEUX LEÇONS STRATÉGIQUES DE LA CRISE GOOGLE CHINE

par François-Bernard Huyghe, chercheur associé à l'IRIS

## I) Technologie et idéologie sont inséparables

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 certes sur des questions techniques :

- l'efficacité et la traçabilité 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 Facebook ou de Twitter et être un pays en plein développement économique et technique ?).

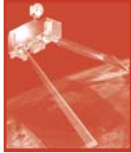
Mais, au-delà de ces questions de technologie, d'ailleurs encore mal résolues, se sont vite révélées des positions idéologiques :

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 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 peccadille 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 renforcer 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 souverain 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 dénoncé 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. ■

*François-Bernard Huyghe est chercheur associé à l'IRIS, Docteur en Sciences Politiques, il est aussi enseignant, écrivain et consultant.*



## Rappel des faits en quelques liens

### Notion de cyberguerre

La théorie de la guerre cybernétique envisagée par les américains est exposée sur Internet. Voir notamment un rapport de commission américaine: [Us-China Economic and Security Review Commission](#). ( voir aussi [cyberattaques](#)).

Les Etats-Unis développent la doctrine de cyberguerre (voir [INEW](#)). [La défense](#) et le renseignement facilités par des moyens *high tech*.

En Juillet 2009, à l'occasion d'attaques contre des serveurs gouvernementaux, financiers et de médias, en Corée du Sud et aux USA, certains ont accusé la [Corée du Nord](#). Avant de diriger les soupçons vers la Chine.

Les Américains ont inauguré en Novembre 2009 le Centre national d'intégration de la cyber-sécurité et des communications ([NCCIC](#)) Et Barack Obama, a nommé un Monsieur [Cybersécurité](#), Howard Schmidt sur [ces questions](#).

Des chercheurs [canadiens](#) de l'Université de Munk pointent depuis mars dernier vers un réseau du nom de [Ghostnet](#), vaste structure d'espionnage électronique située sur le territoire chinois et qui aurait compromis des ordinateurs de services officiels dans spays.

La Chine, est souvent [désignée par les États-Unis](#) comme responsable d'attaques contres les systèmes informationnels, tandis que les *think tanks* de Washington soulignent que ce pays se dote de capacités "cyberguerrières" en accord avec sa doctrine militaire.

### La Chine et Google en pleine cyberguerre ?

Une [cyberguerre](#) entre la Chine et... Google ? Superpuissance contre méga-entreprise ? Celle qui circulait dans la presse vers le milieu de Janvier 2010.

Deux vagues d'attaques sont recensées en Décembre 2009.

La première serait de l'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 à Pékin sur gmail (les adresses électroniques fournies par Google), y compris en Europe, elle pourrait bien ne guère avoir de rapport avec la première.

La Chine est elle coupable ? Rien n'est moins certain. 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 a pu remonter jusqu'à une adresse IP se terminant en "cn") ne veut pas dire par les autorités chinoises.

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'il a subie. Les attaques auraient pu être [relayées par des complicités](#) humaines au sein de Google.

Demandant des explications à la Chine sans vraiment l'accuser, Hillary Clinton a prononcé un [important discours](#), le 21 Janvier 2010 sur la question de la liberté sur Internet, texte où la célèbre revue Foreign Policy voit l'amorce d'une [cyberguerre froide](#).

Derniers développements de ce que certains ont baptisé "[opération Aurora](#)" : - Suite à ses menaces des premiers jours et après avoir [négocié](#) avec les autorités chinoises, Google a décidé de les défier.

La compagnie californienne qui a avait pourtant accepté de censurer [son moteur de recherche en chinois en 2006](#), et dont le chiffre d'affaire s'élève à 24 milliards de dollars, ne perdrait que [300 millions](#) si elle se retirait d'un pays où, de plus, son moteur de recherche est largement dépassé par son rival local : Baidu.

Les relations entre l'Empire du Milieu et la Société du Bien rentrent dans une [nouvelle phase](#). Google vient de détourner son moteur [google.cn](#), vers celui de [Hong Kong](#), également en chinois mais non censuré.

Des sociétés chinoises deviennent, à l'image de leur pays, des géants. Les portails chinois commencent à se hisser au rang des plus visités dans le monde : [baidu.com](#), 3ème, [sina.com.cn](#), 6ème, [sohu.com](#), 8ème et [163.com](#), 9ème 6.

Pékin vient d'annoncer des rétorsions et de baisser le débit de la circulation en direction du site de Hong Kong, et China Mobile et China Unicom ou encore Top Com ont abandonné des projets juteux avec la compagnie américaine.

Google se défend sur son [blog officiel](#). Et dit toujours vouloir se retirer définitivement de Chine le 10 Avril 2010. Google a adhéré à un réseau: [Global Network Initiative](#) pour la liberté de publier sur Internet.

François-Bernard Huyghe

## GLOSSAIRE

**Adresse IP :** Internet Protocol. L'adresse IP est l'authentification de tout matériel relié à un réseau informatique. Elle est spécialement utilisée pour identifier les ordinateurs qui se connectent sur le réseau Internet.

**Algorithme:** Ensemble des règles opératoires propres à un calcul ou un traitement informatique. Les algorithmes permettent à l'information d'agir comme un programme, productrice virtuelle de réalité.

**Cyberattaque:** Se dit d'une attaque menée sur un dispositif informatique. Elle est rendue possible grâce au développement de réseaux cybernétique mondiaux comme Internet. La plus claire démonstration de cyberattaque est le développement de virus sur la toile.

**Cyberguerre:** Ensemble de cyberattaques menées contre un objectif précis. Permet de dérouter volontairement des informations. Guerre virtuelle, elle n'en a pas moins des conséquences très concrètes.

**Cyberterrorisme:** Attaque délibérée par un adversaire militaire ou civil, organisation ou civil contre les systèmes informatiques cruciaux d'un pays pour les contrôler ou les rendre inefficients. Existe surtout sur le papier.

**F.C.C Federal Communication Commission (Etats-Unis):** Equivalent de l'Autorité de Régulation des Télécommunications française.

**Guerre de l'Information :** Toute technique destinée à acquérir des données et connaissances (et à en priver l'adversaire), dans une finalité stratégique. Soit en s'attaquant à ses systèmes (vecteurs et moyens de traitement de l'Information) soit en jouant sur le contenu, en visant une domination informationnelle. Sous son aspect offensif: toute opération recourant à la rumeur, à la propagande, à un virus informatique qui corrompt ou détourne le flux des informations ou données d'un adversaire qu'il soit un Etat, une armée, une entité politique ou économique...

**Hacker:** Nouveaux pirates qui accèdent, via Internet à des sites protégés par jeu ou lucre, y font des prélèvements ou des modifications, copient, vendent ou offrent illégalement des logiciels payants.

**Identifiant:** Etiquette technique permettant de reconnaître l'origine ou la destinations d'une communication électronique. L'identifiant peut représenter un appareil (le numéro d'un téléphone, par exemple) ou le code désignant un utilisateur. Exemples: adresse IP de chaque ordinateur naviguant sur Internet ou l'IMEI de chaque appareil mobile.

**Idéologies:** définition banale de l'idéologie: fumées (idées de l'autre), utopies, délires, rêveries, idées contre-réalité... Définition chic: représentation du Monde apparemment rationnelle (mais partielle et faussée) que se font des acteurs en fonction de leur position et de leurs intérêts (notion qui permet d'expliquer pourquoi, l'idéologie dominante, Ô surprise, domine les médias. Rappel : "une" idéologie, ça n'existe pas. Mais il y a des idéologies, des systèmes d'idées polémiques traduisant des évaluations et visant à des effets concrets. Ils se heurtent à d'autres systèmes et visent à se propager dans d'autres têtes.

**Logiciels espions (Spyware) :** Rapporte à celui qui les implante les activités légitimes de l'utilisateur d'un ordinateur, d'un réseau ou d'un téléphone mobile. Exemple: le logiciel carnivore que le FBI peut installer chez des Fournisseurs d'Accès à Internet pour surveiller les messages électroniques et les consultations d'un suspect.

**Logiciels malveillants (Malware):** Logiciels introduits clandestinement dans un ordinateur ou appareil comparable pour y exercer des actions nocives sans l'accord du propriétaire légitime.

**N.S.A: (National Security Agency):** Agence américaine de renseignements responsable des interceptions de communications (téléphone, Fax, Internet)

**Paquets IP:** façon dont voyagent les données sur Internet, regroupées par "paquets" qui peuvent emprunter des chemins différents mais sont regroupés à l'arrivée

**RMA (Revolution Military Affairs) :** Théorie de développement militaire. Souvent associée à la technologie, aux communications et à l'industrie aérospatiale. Théorie de révolution permanente de la technologie militaire.