

# CONTRÔLER LES « POSITIONS ÉMINENTES » DU CYBERSPACE

LE 30 MARS 2010 PHILIPPE QUÉAU

L'Internet est un domaine public mondial dont la maîtrise est vitale pour les États-Unis, de même que la mer, l'air et l'espace, estime l'armée américaine. Comment la volonté de « domination » se traduit-elle dans le cyberspace ? De façon générale, quelles sont les « positions éminentes » dans la société de l'information et de la connaissance ?

L'Internet est un domaine public mondial dont la maîtrise est vitale pour les États-Unis, de même que la mer, l'air et l'espace, estime l'armée américaine. Comment la volonté de « domination » se traduit-elle dans le cyberspace ? De façon générale, quelles sont les « positions éminentes » dans la société de l'information et de la connaissance ?

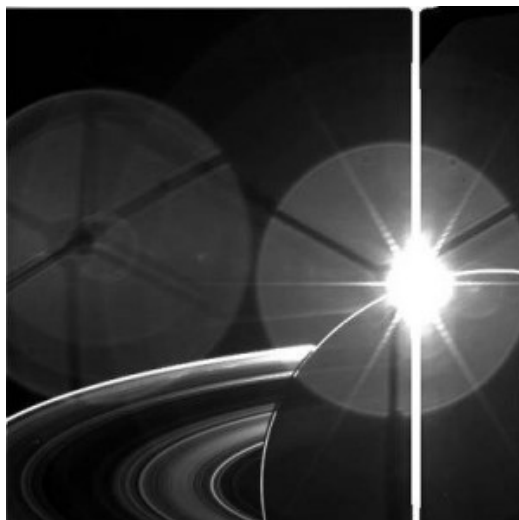
Pour comprendre la nature de la mondialisation à une époque donnée, il peut n'être pas inutile de se référer aux stratégies militaires d'occupation de l'espace global, elles aussi fort caractéristiques et révélatrices des grandes structurations à l'œuvre.

Pour illustrer ce point, je voudrais parler de la question actuelle des « positions éminentes » pour le contrôle des domaines publics mondiaux.

De tout temps, en matière de stratégie militaire, le contrôle des « positions éminentes » a joué un rôle essentiel. La maîtrise des points hauts, ou de l'espace aérien en sont des exemples. De nos jours, il s'agit surtout de s'assurer le contrôle de la « position éminente » suprême : l'espace.

Rappelons qu'il y a environ 1000 satellites actifs actuellement en orbite. La moitié d'entre eux appartiennent aux États-Unis, et ceux-ci sont approximativement pour 50% d'usage civil et pour 50% d'usage militaire. Rappelons aussi que le 21 janvier 1967 un Traité international a banni la nucléarisation de l'espace – mais pas l'usage d'armes conventionnelles dans l'espace. C'est cette réalité que la polémique internationale autour du système de défense antimissile révèle.

Dans le cadre d'une stratégie globale, que l'on a pu qualifier de « pax americana », l'armée américaine a identifié comme d'importance vitale divers domaines publics à l'échelle globale (« global commons ») : la mer, l'air, l'espace et le cyberspace (sea, air, space, cyberspace).



Elle a aussi défini une doctrine stratégique à leur égard, qu'elle a formulée ainsi: « La domination militaire des domaines publics mondiaux est un facteur clé de la position de puissance globale des États-Unis » (“The “command of the commons” is the key military enabler of the US global power position”).

Le contrôle des domaines publics mondiaux signifie que les États-Unis obtiennent beaucoup plus d'usages et d'avantages de la mer, ou de l'espace que les autres puissances, qu'ils peuvent empêcher leur utilisation par celles-ci, et que ces dernières perdraient tout

engagement militaire sur les domaines publics mondiaux si elles cherchaient à en empêcher l'accès aux États-Unis. "Command means that the US gets vastly more military use out of the sea, space and air than do others, that it can credibly threaten to deny their use to others, and that others would lose a military contest for the commons if they attempted to deny them to the US." Barry Posen, *The Military Foundations of US Hegemony*, International Security, Summer 2003, pp. 5-46 .

On trouve aussi formulée une doctrine plus "politique" des domaines publics mondiaux, traduisant de façon fort intéressante l'admission d'un lien structurel entre les « domaines publics » et le « bien commun » mondial. C'est la doctrine selon laquelle : « La stabilité des domaines publics mondiaux est en soi un bien commun » ("Stability within the global commons is a public good").

Tout le monde a en effet un intérêt évident à une « stabilité » des domaines publics. La plupart des pays ont un très grand intérêt à cette stabilité, mais il est aussi vrai que d'autres pays, qui n'en tirent que peu d'avantages directs, restent de par leur degré de développement incapables de tirer tout le parti souhaitable des domaines publics mondiaux.

La puissance dominante, qui en tire des avantages tactiques et stratégiques absolument essentiels, estime en conséquence qu'il lui revient le rôle d'assurer la protection ou la garantie de cette stabilité. La question plus générale de savoir si cette stabilité est mieux garantie sous leur égide, plutôt que par un autre mécanisme, par exemple multilatéral, reste ouverte.

Mais ce qui m'intéresse surtout ici c'est le concept stratégique de « position éminente », dans le contexte plus large des sociétés de la connaissance.

La notion concrète de « position éminente » varie à l'évidence suivant les milieux où l'on opère. La volonté de « domination » (« command ») qui se traduit d'une certaine manière dans l'espace, comment se traduit-elle donc dans le cyberspace ?

Plus généralement, quelles sont les « positions éminentes » dans la société de l'information et de la connaissance ?

On peut avancer par exemple les nœuds de concentration mondiale du trafic Internet, les treize « serveurs racine » du DNS (dotés du système « Carnivore » ou de logiciels d'analyse des données « deep packet inspection »).

Mais il y a aussi le contrôle de l'architecture des réseaux et de ses grandes « autoroutes de l'information » (citons le système d'espionnage Echelon pour les satellites et divers autres systèmes d'espionnage pour les fibres sous-marines). L'architecture logicielle générale, les routeurs (avec les trap-doors), la prééminence dans le domaine des virus et autres chevaux de Troie électroniques, font à l'évidence partie des autres « positions éminentes » dont il s'agit de s'assurer le contrôle. Voir à ce sujet <http://www.eff.org/issues/nsa-spying>.

Naturellement, si j'ose dire, les « domaines publics » de la société de l'information peuvent être « contestés » par d'autres puissances (« contested commons »). L'espace en fait partie.

On cite souvent, à cet égard, le récent tir d'un missile chinois sur l'un de ses propres satellites. Cela a pu être interprété comme un « message » adressé au monde sur la question de l'arsenalisation croissante de l'espace.

Les attaques de cyberguerre (cf l'affaire Google) font partie du même scénario de « contestation des communs ».

Un autre exemple de « communs », à la fois contestés et enchevêtrés (couplant des questions de stratégie militaire globale, et des systèmes clé pour les sociétés d'information): le système GPS, qui se voit concurrencé par le système européen Galileo.


On pourrait utilement chercher d'autres aspects stratégiques du concept de « position éminente » dans le cadre des sociétés de l'information. Ainsi, quel statut donner au renforcement continu de la propriété intellectuelle depuis plusieurs décennies ? (Barrages de brevets, frappes juridiques préemptives). Le non-débat public et démocratique sur l'Accord commercial Anti-Contrefaçon (ACAC ou ACTA en anglais) en fait partie. Font aussi partie de la stratégie du « contrôle des communs », les questions de la captation privative des capitaux cognitifs (Google), sociaux (Facebook), attentionnels (Twitter), humains (marchandisation des données personnelles, observation et de l'exploitation des « intentions » des usagers).

Il faudrait, plus généralement, s'interroger sur le rôle global, stratégique et tactique, des techniques d'appropriation et de domination du domaine public des informations et des connaissances, et les confronter à une réflexion, par ailleurs urgente, sur la nature même de l'intérêt général mondial.

—

> Billet initialement publié sur **Metaxu sous le titre "La position éminente"**

## STÉPHANE BORTZMEYER

le 2 avril 2010 - 15:38  SIGNALER UN ABUS - PERMALINK



*Je n'ai rien contre le fond de l'article mais il y a au moins une erreur énorme qui semble indiquer que l'auteur a tapé sans tourner sept fois son clavier dans sa main.*

*Le texte dit « Les treize « serveurs racine » du DNS (dotés du système « Carnivore » ou de logiciels d'analyse des données « deep packet inspection »). » Il y a une part de vérité (un serveur DNS racine voit venir la requête complète et, de ces interrogations, peut analyser et déduire bien des choses) et beaucoup de baratin. Ainsi, Carnivore ÉTAIT*

*un système d'espionnage du trafic aux États-Unis. Il visait à la détection du CONTENU des messages et n'avait probablement pas de fonctions lui permettant d'analyser les requêtes DNS. Il est théoriquement possible que si, et qu'il ait été déployé près des serveurs DNS gérés par ce pays, par exemple ceux de l'armée états-unienne mais rien n'indique qu'il ait été installé sur tous les serveurs racine, notamment ceux gérés par des pays étrangers. Même sur les sites Web les plus complotistes, je n'ai pas vu d'informations là-dessus. Soit Philippe Quéau a des informations précises (et il faudrait les publier), soit c'est juste pour faire joli.*

*Encore pire, l'allusion au DPI (« deep packet inspection »). Le DPI est une technique (utilisée notamment par certains FAI, avant le filtrage ou la limitation de trafic) pour déterminer le « vrai » protocole utilisé par un trafic donné, lorsque celui-ci a été délibérément obscurci (par exemple en faisant passer du SSH par le port 443 pour qu'il profite des filtres acceptant le HTTPs). Quel pourrait bien en être l'intérêt pour des serveurs racine, qui reçoivent des requêtes EN CLAIR ?*

*Bref, la crédibilité de l'article serait améliorée en supprimant ce genre d'affirmations infondées et bien légères. On a le droit de ne pas connaître en détail la technique mais, dans ce cas, on évite de lancer des gros termes techniques pour impressionner le lecteur.*

VOUS AIMEZ



0

VOUS N'AIMEZ PAS



0

LUI RÉPONDRE

### 1 ping

Les tweets qui mentionnent Owni Contrôler les « positions éminentes » du cyberspace -- Topsy.com le 30 mars 2010 - 11:34

[...] Ce billet était mentionné sur Twitter par damien douani, Owni, Alexandre Ultré, Alice, Guilbert et des autres. Guilbert a dit: RT @Own1: #Owni Contrôler les « positions éminentes » du cyberspace <http://bit.ly/c7ocsC> [...]

[WORDPRESS HASHCASH] The comment's actual post text did not contain your blog url (<http://owni.fr/2010/03/30/controler-les-%c2%ab-positions-eminentes-%c2%bb-du-cyberspace>) and so is spam.