LES ACTIVITÉS D'ESPIONNAGE ÉLECTRONIQUE ET DE CONTRÔLE D'INTERNET À L'ÈRE DE L'INFONUAGIQUE : LE CAS DE LA CHINE

Par **Nir Kshetri**, Professeur adjoint, University of North Carolina at Greensboro, États-Unis • kshetri1@hotmail.com
Traduit de l'anglais

RÉSUMÉ Même si environ quarante gouvernements contrôlent leur environnement virtuel, peu ont réussi à le faire aussi bien que la Chine. Au cours des dernières années, cette réalité est devenue préoccupante en raison de la diffusion et du développement rapide de l'infonuagique, lequel est décrit comme « le » mécanisme d'espionnage par excellence. Dans cet article, nous proposons un cadre qui permet de définir des contextes clairs et des mécanismes associés aux mesures de contrôle des régimes autoritaires. Nous développons le concept de champ institutionnel formé autour du contrôle d'Internet dans les régimes autoritaires. Le fait de considérer le cybercontrôle comme un champ institutionnel nous permet de nous pencher sur l'évolution des institutions cognitives, normatives et régulatrices. Nous proposons un modèle qui explique la façon dont un champ institutionnel évolue.

ABSTRACT Although about forty governments control their online environments, few have done so more skilfully than China. This concern has become especially pronounced in recent years due to a rapid diffusion and development of cloud computing, which is described as the ultimate spying machine. In this paper, I propose a framework for identifying clear contexts and the attendant mechanisms associated with authoritarian regimes' Internet control measures. I build on the concept of an institutional field formed around Internet control in authoritarian regimes. Viewing cyber-control as an institutional field enables me to examine the evolution of regulative, normative and cognitive institutions. I advance a model that explains how an institutional field evolves.

Pour citer cet article : Kshetri, N. (2012). « Les activités d'espionnage électronique et de contrôle d'Internet à l'ère de l'infonuagique : le cas de la Chine », *Télescope*, vol. 18, n° 1-2, p. 169-187.

Bien qu'une quarantaine de gouvernements contrôlent leur environnement virtuel, l'approche de la Chine représente probablement le contrôle le plus sophistiqué du cyberespace. En ce qui concerne les technologies de l'information et de la communication (TIC), les stratégies de l'État chinois visent à trouver un équilibre entre modernisation économique et contrôle politique (Kalathil, 2003). Selon Reporters sans frontières, la Chine a été l'un des premiers pays à réaliser qu'elle ne pourrait se priver d'Internet et que celui-ci devait dès lors être contrôlé (McLaughlin, 2005). On peut donc avancer que Beijing[1] a fixé son attention sur

[1] On peut utiliser *Pékin* ou *Beijing* pour désigner la capitale de la Chine et, par extension, le gouvernement chinois. [NDT]

Internet avant d'autres pays en développement parce qu'il a eu besoin de conserver sa mainmise sur le pays (Yang, 2001). Des dizaines de milliers d'agents gouvernementaux seraient engagés dans diverses activités de cybercontrôle (Stevenson-Yang, 2006). En 2007, le gouvernement chinois a d'ailleurs ordonné la fermeture de 44 000 sites Web ; quelque 868 personnes ont été arrêtées sur des chefs d'accusation de cyberpornographie et environ 2 000 individus impliqués dans des activités relatives à la cyberpornographie ont été pénalisés (E-Commerce Times, 2008). Selon Reporters sans frontières, 50 « cyberdissidents » chinois étaient en prison en janvier 2008 (Jesdanun, 2008). De nouvelles dispositions réglementaires obligent les fournisseurs de vidéos sur Internet à censurer tous les clips ayant un contenu « anti-Beijing » (Einhorn, 2008). En décembre 2011, la Chine a resserré ses règlements en exigeant des microblogueurs qu'ils s'inscrivent à ces services en utilisant leurs noms réels. De telles dispositions ont été qualifiées de « mesures de censure sans précédent » par Reporters sans frontières.

Depuis 2009, le gouvernement chinois a également resserré les exigences en matière d'enregistrement et les étapes en vue d'obtenir un nom de domaine se terminant par « .cn ». Les sociétés souhaitant s'enregistrer doivent soumettre une copie de leur licence. Par ailleurs, les autorités chinoises ont réussi à obtenir de compagnies étrangères du secteur des technologies, dont Yahoo!, Google et Microsoft, des ententes en vue de filtrer et de dépister les mots jugés problématiques (French, 2006 ; McLaughlin, 2005). En plus de ses effets sociaux et politiques, le contrôle que le gouvernement exerce sur Internet a également constitué un problème majeur pour la croissance du commerce électronique en Chine (Kshetri, 2007).

Les problématiques associées au cybercontrôle du gouvernement chinois se sont complexifiées au fil des ans et l'infonuagique a connu un déploiement et une diffusion rapides. Il importe de savoir que certaines compagnies chinoises figurent parmi les joueurs les plus influents du marché mondial de l'infonuagique (Kshetri, 2011). Selon la firme CCID Consulting, le marché chinois de l'infonuagique, qui a enregistré un chiffre d'affaires de 1,5 milliard de dollars américains en 2009, devrait atteindre les 10 milliards de dollars américains en 2012, et le « nuage » est décrit comme « le » mécanisme d'espionnage par excellence (Kshetri, 2010a). Un des dangers évidents dans un régime autoritaire provient de la possibilité que le gouvernement intensifie ses contrôles sur les citoyens en utilisant cette technologie (Zittrain, 2009). Selon une enquête de Foreign Policy, 38 % des experts mondiaux d'Internet considèrent que le gouvernement constitue la plus grande menace à Internet ouvert, 34 % des experts estiment que ce sont les sociétés privées qui représentent la plus grande menace et 15 % d'entre eux ont pointé les cybercriminels (Foreign Policy, 2011).

Afin de bien saisir les risques liés à la sécurité du « nuage », on peut se référer à l'annonce faite par Google en 2009 qui avait découvert des cyberattaques sur ses infrastructures provenant de la Chine. La compagnie a également constaté que ces attaques faisaient partie d'une vaste opération ayant infiltré les infrastructures d'au moins vingt autres grandes compagnies et d'autres rapports ont montré que des pirates avaient attaqué les réseaux de plus de cent compagnies (McMillan, 2010). En avril 2010, des chercheurs basés aux États-Unis – et au Canada – ont publié

un rapport d'enquête sur un réseau d'espionnage électronique qu'ils ont nommé le Shadow Network (Information Warfare Monitor et Shadowserver Foundation, 2010). Parmi les cibles du réseau figuraient le ministère indien de la Défense, les Nations Unies et le Bureau du dalaï-lama. On peut lire dans ce rapport : « *Clouds provide criminals and espionage networks with convenient cover, tiered defenses, redundancy, cheap hosting, and conveniently distributed command and control architectures*. » On a également fait état, en 2009, d'une opération de cyberespionnage venant de la Chine, connue sous l'appellation GhostNet, qui aurait infecté 1 295 ordinateurs dans 103 pays (Hvistendahl, 2010).

Les questions liées au contrôle du cyberenvironnement par les régimes autoritaires sont fondamentales pour les intérêts et les objectifs de toute une gamme d'acteurs, comme les gouvernements occidentaux, les groupes de défense des droits de la personne (par exemple, Amnistie internationale), les groupes dissidents chinois, le Falun Gong[2], les groupes anti-Falun Gong et des sociétés faisant partie de la chaîne de valeur d'Internet. Plus important encore peut être le fait que parmi ces acteurs, qui tendent à avoir des intérêts concurrentiels et des raisons d'être disparates (Brint et Karabel, 1991), la balance du pouvoir et les structures d'interactions se dégradent rapidement dans le temps. De nouvelles organisations ou populations font leur entrée dans les dialogues entourant le cybercontrôle et d'autres en sortent (Hoffman, 1999).

D'un point de vue de la théorie, du management et de la politique, il est important d'avoir une compréhension fine des mesures du contrôle d'Internet dans les régimes autoritaires. Premièrement, la relation entre la diffusion d'Internet et la croissance de la démocratie est incertaine (Wilson et Segal, 2005) : le lien entre diffusion d'Internet et démocratie, surtout dans les régimes autoritaires, semble être moins défini que ce qu'il paraît de prime abord. Il existe, d'une part, des raisons favorables et défavorables, toutes bien fondées, quant à la participation des compagnies occidentales dans des activités liées à Internet dans des régimes autoritaires et, d'autre part, on compte un nombre considérable d'opinions mal informées et insoutenables sur le sujet. Par exemple, lorsque la compagnie de téléphonie française Alcatel a entamé des pourparlers avec Lucent en 2006 en vue d'une fusion, certains décideurs américains ont critiqué les liens d'Alcatel avec l'Iran, car Alcatel avait amélioré le réseau téléphonique d'Iran et avait fourni au pays des connexions DSL pour Internet haute vitesse (Bremmer, 2006). Certains ont donc argué qu'Alcatel avait aidé le régime iranien. Néanmoins, d'autres peuvent croire le contraire, dans la mesure où le fait d'installer ces structures a permis aux Iraniens de communiquer plus facilement entre eux et avec des personnes à l'extérieur du pays et, par conséquent, a permis de promouvoir la démocratie dans le pays. Pourquoi la relation entre la diffusion d'Internet et la démocratie est-elle si peu claire ? Cela dépend des circonstances. Est-ce qu'Internet force les régimes autoritaires à promouvoir la démocratie ou est-ce qu'Internet sera contrôlé comme les autres médias de masse (Hachigian, 2001 ; Stevenson-Yang, 2006) ? Cette question

[2] Le Falun Gong est un mouvement spirituel chinois. [NDLR]

incontournable d'ordre politique et théorique touche aux préoccupations sociales et politiques plus larges de la société démocratique.

Avant de commencer, il s'avère essentiel de définir quelques notions. L'informatique en nuage, ou infonuagique, consiste à héberger des applications sur les serveurs et à fournir des logiciels et des services par Internet. Dans ce modèle, les entreprises peuvent accéder à la puissance informatique et aux ressources sur le « nuage » et paient pour les services selon leur utilisation (Kshetri, 2011).

Dans cet article, nous ferons tout d'abord une revue des bases théoriques sur le sujet. Nous transposerons ensuite les théories dans le contexte et les limites du cybercontrôle en Chine. Puis, nous discuterons des réactions des acteurs institutionnels par rapport au contrôle d'Internet en Chine. La section finale présente les conclusions et les répercussions.

■ LA BASE THÉORIQUE

Au cœur de notre argumentaire se trouve le concept de « champ » formé autour du cybercontrôle. Hoffman (1999, p. 352) affirme que ce champ est « *formed around the issues that become important to the interests and objectives of specific collectives of organizations* ». Ces organisations comprennent les régimes autoritaires qui tentent de contrôler Internet, les groupes de défense des droits de la personne comme Amnistie internationale, les gouvernements occidentaux, les associations professionnelles et les sociétés faisant partie de la chaîne de valeur d'Internet.

Il faut garder à l'esprit que ces champs ont une nature « évolutive » plutôt que « statique » (Hoffman, 1999, p. 352). Les théoriciens exposent une théorie fascinante sur la façon dont un champ évolue : un champ organisationnel est un système dynamique caractérisé par les entrées et sorties d'organisations et de populations, et/ou les dynamiques d'interactions entre elles (Brint et Karabel, 1991). Tout comme les autres champs « axés sur les enjeux », le contrôle d'Internet peut être vu comme un « espace de jeux de pouvoir » (Brint et Karabel, 1991, p. 355) dans lequel différents acteurs et parties prenantes ayant des intérêts concurrentiels et des objectifs disparates négocient selon leur interprétation de l'enjeu et s'engagent dans une guerre institutionnelle (White, 1992). L'évolution institutionnelle prend donc la forme d'une altération des dynamiques d'interactions et d'un rapport de force parmi les organisations (Hoffman, 1999).

Comme nous l'avons expliqué précédemment, le contrôle d'Internet dans les régimes autoritaires n'est pas encore institutionnalisé, car il n'est ni « accepté sans critique » ni considéré comme une entente « naturelle et appropriée » (Tolbert et Zucker, 1996). Oliver (1991, p. 151) soutient que les réponses stratégiques aux processus institutionnels de plusieurs acteurs institutionnels varient de « la passivité à la résistance active de plus en plus forte : connivence, compromis, évitement, défiance et manipulation ». Ainsi, en Chine les réponses des compagnies Internet à la pression exercée par le gouvernement pour créer un cyberenvironnement contrôlé varient considérablement. De plus, certaines organisations ont changé leurs stratégies de gestion des pressions gouvernementales. Parmi les sociétés étrangères affiliées, Yahoo! a adopté la stratégie de l'acquiescement dès le début,

obéissant aux normes et aux lois et coopérant avec le gouvernement. En revanche, certains portails et moteurs de recherche, tels Google et AltaVista, ont résisté activement à de tels processus ou les ont « défié » pour, au final, être bloqués au pays (Singer, 2002). En d'autres mots, ils sont sortis du champ du cybercontrôle chinois en 2002. Subséquemment, toutefois, les autorités chinoises ont réussi à obtenir de Google des ententes en vue de filtrer et de dépister les mots dits problématiques (French, 2006). Par exemple, la fenêtre de Google fermait automatiquement lorsqu'un internaute utilisait des mots dits problématiques (McLaughlin, 2005). Google est ainsi entré dans le champ du cybercontrôle chinois, mais le cyberenvironnement chinois, défavorable du point de vue de la sécurité, a mené une fois de plus au retrait de Google en 2010.

■ LE CYBERCONTRÔLE EN CHINE

La nature des institutions régulatrices

L'accent mis sur le maintien d'une poigne solide sur la vie et la conscience publiques

Pour les autorités chinoises, il existe une panoplie de raisons pour engager des poursuites et punir les individus pour des « crimes » Internet, par exemple pour protéger la valeur des actifs chinois qui sont exposés aux marchés des capitaux mondiaux ou pour empêcher la formation d'organisations politiques illégales (Stevenson-Yang, 2006). La cyberpolice chinoise a d'ailleurs intensifié ses poursuites pour violations de contenu Internet et un certain nombre de militants prodémocratie, de défenseurs des droits de la personne, de membres du Falun Gong, d'universitaires et d'autres dissidents ont été arrêtés pour leur participation alléguée à des crimes Internet (Hachigian, 2001).

En effet, pour la Chine la loi est marginalisée et le système légal est relégué à un rang inférieur du spectre des mécanismes de médiation et peut en même temps être manipulé par des secteurs puissants au sein de l'État et la société en général (Myers, 1996, p. 188). C'est encore plus vrai dans le cas des lois qui régissent le contrôle d'Internet. La plupart des dispositions réglementaires concernant Internet sont des indications et ne constituent pas des lois formelles (Shie, 2004). Stevenson-Yang (2006) écrit :

> *Published regulations are convenient as a means of expressing policy, but in the end, political policy, not statute, is the true law of the land in China. The case against editors from Southern Metropolis News in 2004 provides an example: the three were convicted of bribery and embezzlement, but their real offenses, it was universally believed, were reporting on Severe Acute Respiratory Syndrome, or SARS [on the internet].*

Comparativement aux autres pays en développement, la Chine a été lente à élaborer des lois pour reconnaître les signatures numériques et électroniques (Aldrich, 1999). Les logiciels de chiffrement des données, qui sont une composante essentielle de la signature numérique, permettent d'envoyer des messages

confidentiels rendant ainsi difficile, voire impossible, pour le gouvernement d'y détecter le contenu politiquement et culturellement répréhensible qui est transmis sur Internet (Kshetri et Dholakia, 2001).

Le cybercontrôle en Chine est par conséquent caractérisé par le manque de règlements et de politiques claires. Au début de 2002, plusieurs moteurs de recherche étrangers, plus particulièrement Google et AltaVista, ont été bloqués pendant plusieurs jours sans aucune explication (BBC News, 2002a et 2002b ; Weaver, 2002). Mettant en relief les problèmes vécus par les organisations causés par le manque de clarté, un regroupement de gens d'affaires a demandé au gouvernement chinois de fournir des dispositions réglementaires plus précises (Kalathil, 2003). Stevenson-Yang (2006) écrit :

> *International companies may or may not agree with this set of prohibitions, but they do not generally object to them. Rules, as long as they are knowable and actionable, are easily accepted as a sovereign nation's prerogative. But the heart of China's information control system lies in the prescriptive regime – the one designed to manage the process of creating public speech and, above all, designed to ensure that public speech does not have damaging effects.*

L'intervention de l'État dans l'économie facilitant les contrôles

En Chine, l'intervention de l'État dans l'économie (Pei, 2006) facilite sa surveillance des mesures de contrôle d'Internet. En 2001, 70 % des entreprises de grande et de moyenne taille transformées en sociétés comptaient des membres du Parti communiste au sein de leur conseil de direction (Pei, 2006) et les fournisseurs de services Internet sont contrôlés par des sociétés d'État (McLaughlin, 2005). La Chine utilise donc sa propriété ainsi médiée pour tirer des bénéfices économiques d'Internet et dans le même temps pour combattre les risques qu'il représente (Hachigian, 2001). Un groupe au sein du ministère de l'Industrie de l'information coordonne les efforts pertinents du gouvernement pour détecter des contenus répréhensibles et par la suite mettre en œuvre un barrage. Pour créer le barrage, le groupe envoie l'information aux neuf sociétés d'État fournisseurs d'accès Internet qui contrôlent le trafic en ligne de la Chine (Stevenson-Yang, 2005).

Dans l'industrie des télécommunications sans fil, 70 % des opérateurs de télécommunication appartiennent à l'État (Zhang et Prybutok, 2005). Comparativement à l'Occident, les compagnies de technologies chinoises sont plus centrées sur l'État et moins sur le client. Des arguments de poids existent pour étayer la notion voulant que les priorités de l'État aient préséance sur les profits des actionnaires des compagnies de télécommunications chinoises (Kshetri, Palvia et Dai, 2011).

La croissance des capacités gouvernementales en technologies de l'information et de la communication

Afin d'accroître l'efficacité des activités de surveillance, le gouvernement chinois a également augmenté ses capacités en TIC. Pendant que la Chine assujettit le réseau pour usage gouvernemental (Hachigian, 2001), le rendement de son gouvernement électronique est qualifié de plus avancé que celui de pays

industrialisés comme la Suisse, le Royaume-Uni, Singapour et l'Allemagne (West, 2002). Dans ses activités de gouvernement électronique, le gouvernement chinois a recours à de nombreux outils des TIC, comme la messagerie texte, et dans certains cas ces outils sont en train de remplacer certains médias plus traditionnels (Kshetri, Dholakia et Awasthi, 2003).

Selon certains rapports, des dizaines de milliers d'agents gouvernementaux feindraient d'être des dissidents et participeraient aux conversations sur les sites de clavardage, parlant contre le gouvernement. Par conséquent, nombreux sont les internautes qui craignent de participer à des conversations en ligne sur des sujets comme la démocratie, le Japon, la religion et autres questions délicates (Stevenson-Yang, 2006) : la Chine possède le plus grand corps de police Internet au monde (Mallaby, 2006).

Jusqu'à la fin des années 1990, le barrage Internet prenait principalement la forme d'une interdiction d'accès à certains sites. Par la suite, l'accès à ces sites a été rétabli, mais il était impossible de mener à bien des recherches dont les mots clés étaient associés à des « questions délicates ». Selon le Berkeley China Internet Project, le gouvernement cache les sites qui contiennent des termes tels que « liberté », « démocratie », « Chine libérale » et « Falun » (Foushee, 2006).

Le découplage des actions substantielles et symboliques

Les institutions régulatrices sont également caractérisées par le découplage d'actions substantielles et symboliques. Un fonctionnaire qui supervise les affaires Internet pour le Conseil d'État de la Chine a déclaré que les efforts déployés par la Chine en vue de réguler les contenus Web visaient principalement la pornographie ou d'autres contenus dommageables pour les adolescents et les enfants (Kahn, 2006). Or, malgré le fait que la pornographie soit illégale, son accès n'est pas bloqué (Los Angeles Times, 1997).

Beijing découple également les mesures illégitimes de contrôle d'Internet des structures formelles. Il faut savoir que les réponses des organisations aux pressions des institutions ne sont pas toujours légitimes. Par exemple, l'étude réalisée par Elsbach et Sutton (1992, p. 716) indiquait que les organisations activistes découplaient les actions illégitimes des structures organisationnelles formelles en perpétrant ces actions en tant qu'individus anonymes ou en tant que membres d'un groupe temporaire opérant sous différents noms. Comme les régimes autoritaires tendent à faire moins de contrôles et de bilans que les démocraties pour prévenir l'abus de pouvoir (Popov, 2006 ; Stoner-Weiss, 2006), ces régimes sont susceptibles d'être engagés dans des mesures illégitimes de contrôle d'Internet. De plus, en raison de l'anonymat inhérent à Internet, il est facile de découpler des mesures illégitimes de contrôle d'Internet des structures formelles. Selon des rapports d'événements, les autorités chinoises vont jusqu'à envoyer des virus pour attaquer les sites bannis (Guillén et Suárez, 2005).

La nature des institutions normatives

Les associations professionnelles et commerciales sont d'importantes catégories d'institutions normatives. Une profession est autoréglementée par un code

d'éthique (Claypool, Fetyko et Pearson, 1990) et caractérisée par son rôle en tant que communauté morale (Camenisch, 1983). Les codes prescrivent aux membres d'adopter des normes de conduite plus élevées que ce que la loi commande (Backoff et Martin, 1991) afin de rendre les normes professionnelles visibles (Frankel, 1989), de garantir au public et aux clients que les membres sont compétents et intègres et de maintenir et renforcer de hauts standards (Ward et autres, 1993).

Les associations professionnelles chinoises qui font partie des institutions normatives liées au secteur du cybercontrôle semblent posséder des caractéristiques idiosyncrasiques et inutiles. Soutenue par le gouvernement, la Société Internet de Chine (Internet Society of China – ISC), formée en mai 2001 et comptant plus de 130 membres, en est un exemple frappant. L'ISC est parrainée par les entreprises d'accès réseau, les fournisseurs de services Internet, les fabricants d'équipements et les instituts de recherche. Sa constitution peut être vue comme une partie de la stratégie de manipulation de Beijing, soit « une tentative dirigée et opportuniste de coopter, d'influencer ou de contrôler les pressions institutionnelles et les évaluations » (Oliver, 1991, p. 157). Des recherches indiquent que pour accroître leur influence, des organisations comme l'ISC peuvent tenter de persuader des responsables d'organisations de se joindre à leur organisation ou de siéger à leur conseil de direction (Oliver, 1991, p. 157). L'ISC, par exemple, a demandé aux compagnies Internet de signer une déclaration volontaire portant sur « l'autodiscipline de l'industrie Internet de Chine » qui oblige ces dernières à enquêter sur les sites Web ayant un contenu politique et culturel dit problématique et à en bloquer l'accès. En mars 2002, la déclaration était signée par plus de 120 portails Internet (Stout, 2002). La déclaration oblige les signataires à ne pas disséminer d'information qui peut constituer une menace pour la sécurité de l'État ou la stabilité sociale (Economist, 2002). Ainsi, en 2009, le moteur de recherche le plus populaire en Chine, Baidu, et dix-neuf autres compagnies Internet ont reçu de Beijing le « prix de l'autodiscipline pour Internet ». Les agents de l'ISC ont encensé ces compagnies pour le rôle qu'elles ont joué dans la prise en charge et la consolidation d'un « développement harmonieux et sain » d'Internet (MacKinnon, 2012). Le gouvernement chinois a mis l'accent sur l'importance d'un cyberespace sain et harmonieux. Dans le contexte chinois, un cyberespace *sain* signifie qu'il est exempt de « pornographie » et de « criminalité », et *harmonieux* signifie qu'il ne menace pas l'ordre social et politique de l'État contrôlé par le Parti communiste de Chine, ni ne le remet en question.

Les activités de l'ISC diffèrent radicalement de celles d'associations professionnelles du secteur du commerce électronique d'Occident. Par exemple, la UK Mobile Marketing Association a publié son code de conduite en décembre 2003, lequel précise à quels moments du jour les marchands de produits sans fil peuvent cibler les consommateurs (Precision Marketing, 2003). De la même façon, aux États-Unis, au début de 2001 des lobbyistes de l'industrie des technologies et des militants pour la protection des droits des consommateurs et des libertés civiles, dont l'American Civil Library Association, l'Electronic Privacy Information Center et la Consumer Federation of America, ont adressé une lettre aux membres

du Congrès et au président leur demandant de renforcer les règles de protection de la vie privée (Benson et Simpson, 2001). Alors que ces activités sont destinées à protéger la vie privée des consommateurs, les actions de l'ISC ont fait la promotion des intérêts du gouvernement. Par exemple, Hu Qiheng, le président de l'ISC, a décrit le cybercrime comme englobant « les actions allant à l'encontre des intérêts du gouvernement chinois » (Crampton, 2006).

L'une des conséquences d'une société civile faible et d'un gouvernement puissant est que les associations commerciales et professionnelles seront portées à s'engager dans des activités qui respectent l'ordre du jour politique autoritaire du Parti communiste de Chine. Par exemple, l'ISC a annoncé qu'elle aiderait à renforcer l'orientation axée sur la cybersécurité des usagers et des compagnies Internet. Si les actions passées de l'ISC peuvent servir d'un quelconque indicateur, ses activités sont plus susceptibles d'être dictées par le besoin du Parti communiste de Chine de maintenir son pouvoir.

Le gouvernement des États-Unis semble préoccupé par le fait que les secteurs privé et public aient travaillé de concert pour développer des capacités en matière de cyberattaque. Selon un câble diplomatique américain diffusé par WikiLeaks, de juin 2002 à mars 2003, le premier fournisseur de Chine en matière de sécurité de l'information, Topsec, aurait engagé Lin Yong, le fondateur de Honker Union of China (aussi connue sous l'appellation Red Hackers), en tant qu'ingénieur principal de maintenance des services de sécurité afin qu'il supervise la formation (Espiner, 2010). Topsec a en partie été financé par le gouvernement chinois et on dit qu'il assurait la formation et fournissait des services de maintenance à l'ALP[3] (Keizer, 2010).

En Chine, les groupes d'intérêts particuliers et les organisations non gouvernementales sont faiblement organisés (Li, Lin et Xia, 2004) et ils ont peu de marge de manœuvre pour influencer la législation nationale (Su et Yang, 2000) et transformer les structures et les pratiques au sein des entreprises locales (Shen, 2005). Il est également important de différencier les mesures de sécurité Internet des sociétés privées chinoises de celles d'autres pays. En Inde, la National Association of Software and Service Companies a joué un rôle crucial dans le renforcement des établissements liés à la cybersécurité (Kshetri, 2010b). En Chine, les acteurs du secteur privé ont été absents des processus de renforcement de la cybersécurité. Cette tendance distinctive peut être expliquée par l'existence d'un État puissant et d'une société civile faible.

Afin de mieux comprendre le rôle des organisations dans les mesures de contrôle d'Internet, il est possible d'établir un parallèle avec le nationalisme chinois. Pei (2003) a dénombré plusieurs dimensions du nationalisme, y compris ses sources et ses bases. En ce qui concerne ses sources, il avance qu'un certain nationalisme est un produit du volontarisme fondamental (comme le nationalisme aux États-Unis), tandis qu'un autre type de nationalisme est promu par les élites

[3] Sigle de l'Armée de libération populaire de Chine. [NDT]

gouvernementales et encouragé par l'appareil étatique (police, armée, médias gouvernementaux). Le nationalisme chinois est perçu comme étant parrainé par l'État et comme une tentative de remplir un « vacuum idéologique » laissé par un socialisme de plus en plus vacillant (Christensen, 1996 ; Sautman, 2001). Les organisations qui appliquent les mesures de contrôle d'Internet ne manifestent pas un « ensemble de motivations autodirigées » comme ce fut le cas de la réponse de l'industrie des produits chimiques américaine à l'environnementalisme (Hoffman, 1999).

Trois autres facteurs clés suggèrent fortement que les institutions normatives liées au cybercontrôle en Chine tendent à centrer leurs activités sur le gouvernement plutôt que d'opérer selon des « motivations autodirigées » (Hoffman, 1999). Premièrement, comme avancé précédemment, l'établissement profond de l'État dans l'économie soulève la possibilité intéressante que le gouvernement puisse jouer un rôle déterminant (Pei, 2006). Deuxièmement, pour avoir du succès dans le commerce électronique en Chine, les sociétés doivent ouvrir la porte aux agents de l'État et aux hauts fonctionnaires (Einhorn, Webb et Engardio, 2000). La plupart des dispositions réglementaires concernant Internet ne sont que des directives et elles n'ont pas force de loi (Shie, 2004). Le vide réglementaire rend ainsi important le fait d'entretenir de bonnes relations avec les représentants du gouvernement. Pour les organisations de l'industrie du commerce électronique, il est donc primordial de prendre en compte les intérêts du gouvernement. Troisièmement, les concepts de service à la clientèle et de vie privée, qui sont au centre des préoccupations des associations professionnelles liées au commerce électronique dans la plupart des régimes démocratiques, ne sont pas bien implantés dans les régimes autoritaires. Terrill (2005) va encore plus loin, en avançant que « parce que la Chine demeure un État autoritaire, nous ne pouvons pas savoir ce que le peuple chinois désire ». Les sociétés du secteur du commerce électronique chinois subissent donc peu ou pas du tout de pression concernant le service à la clientèle et le respect de la vie privée.

La nature des institutions cognitives

Il est important de comprendre les comportements et les schèmes mentaux des citoyens chinois et des dirigeants d'entreprise. Par exemple, Yahoo! a défendu sa décision de communiquer des informations sur un journaliste, Shi Tao, en arguant que la compagnie ne faisait que suivre les « coutumes » de la Chine (Stevenson-Yang, 2006). Dans le même ordre d'idées, la société chinoise accepte conditionnellement la domination de la société civile par un État puissant. Les analystes avancent que le fait que la génération « post-Tian'anmen » chinoise ait vécu peu ou pas de difficultés a rendu cette génération indifférente à la démocratie (Hvistendahl, 2009).

L'acceptation tacite du cybercontrôle et des activités qui lui sont liées n'est pas hautement établie. Comme nous l'avons énoncé précédemment, il existe des opinions favorables et défavorables à la participation de compagnies occidentales dans le réseautage des régimes autoritaires. Dans le même ordre d'idées, l'acceptation tacite du cybercontrôle n'est pas homogène. Par exemple, tandis que les pro-

pos tenus par le P.-D. G. de Yahoo!, Jerry Yang, et le président de l'ISC, Hu Qiheng, reflètent la croyance selon laquelle le contrôle d'Internet est conforme à la culture chinoise, d'autres ne partagent pas le même avis. Plusieurs observateurs étrangers n'ont jamais été convaincus que la décision de Yahoo! de remettre en question des renseignements sur le journaliste avait quelque chose à voir avec les « coutumes » chinoises (Stevenson-Yang, 2006).

L'évolution de sociétés concurrentielles

Les organisations et les populations qui occupent le domaine du cybercontrôle de la Chine sont aussi touchées par d'autres règles formelles et informelles. Par exemple, des compagnies œuvrant contre la censure tel Freegate (Fowler, 2006) et des multinationales des technologies comme Google, Yahoo! et Microsoft, qui sont des acteurs majeurs du cybercontrôle en Chine, sont basées aux États-Unis. Le domaine du cybercontrôle en Chine est par conséquent influencé par des sociétés concurrentes aux États-Unis qui doivent être analysées afin d'avoir une meilleure compréhension de celui-ci. Hoffman note : « *To fully appreciate the complexity of institutional dynamics, one must analyze specific institutions at the center of an issue-based field and the competing institutions that may lie within the populations (or classes of constituencies) that inhabit that field* » (Hoffman 1999, p. 352).

L'évolution des institutions chinoises centrées sur le cybercontrôle a aussi engendré des changements au sein d'entreprises concurrentes. Par exemple, l'organisation non gouvernementale new-yorkaise Human Rights in China a octroyé des fonds à des entreprises qui œuvrent contre la censure comme Freegate (Fowler, 2006). De la même façon, Amnistie internationale a accusé des compagnies Internet basées aux États-Unis, comme Google, Microsoft et Yahoo!, d'avoir violé la Déclaration universelle des droits de l'homme en acceptant de collaborer avec le gouvernement chinois pour censurer l'utilisation d'Internet en Chine (US Federal News Service, 2006). Aux États-Unis, la promulgation de la Global Online Freedom Act 2006 a renforcé les pouvoirs que le gouvernement des États-Unis exerce sur les compagnies technologiques. L'évolution des institutions formelles et informelles dans les pays occidentaux a donc reconstruit le domaine institutionnel du cybercontrôle en Chine.

■ DISCUSSION

La nature des mesures de contrôle d'Internet du gouvernement chinois

On peut soutenir que la résilience du Parti communiste de Chine est attribuable à une combinaison de réformes et de croissance économique (Guoguang, 2006; Marsh et Dreyer, 2003). Plus directement, le Parti communiste compte sur l'économie de l'information pour améliorer son image et il s'attend à ce qu'une économie plus prospère et axée sur les technologies puisse accroître le respect qu'il inspire (Kshetri et Cheung, 2002). En résumé, la Chine souhaite promouvoir la nouvelle économie afin de tirer profit des bénéfices économiques d'Internet.

Hachigian (2001) cite un haut fonctionnaire : « Nous, au gouvernement, pensons que nous avons raté une bonne partie de la révolution industrielle. Et nous ne voulons pas rater cette révolution-ci. »

En cette matière, la Chine a démontré une certaine volonté de former une alliance étonnante avec son grand rival, Taïwan. Elle est aussi en train de desserrer ses restrictions quant à son approche du cybercontrôle. En juin 2011, elle a annoncé un investissement de 154 millions de dollars américains pour mettre sur pied un centre de l'infonuagique pour les sociétés technologiques et de jeunes entreprises à Chongqing. La région administrative spéciale de l'infonuagique ne sera pas soumise aux filtres sévères de censure du pays (Russell, 2011). La Chine cherche également à conclure des partenariats avec des fabricants taïwanais de différents domaines de l'infonuagique (Wang, 2011).

À la fin des années 1990, les techniques de contrôle d'Internet en Chine étaient moins « affûtées ». Les usagers devaient s'inscrire à leur bureau local de sécurité, permettant ainsi aux fonctionnaires de savoir avec certitude qui visitait quel site (Rodan, 1998). Dans ses efforts pour promouvoir la nouvelle économie, cette stratégie a par la suite changé. Selon un rapport de Reporters sans frontières, le contrôle d'Internet en Chine est mené selon un « savant mélange d'investissements, de technologie et de diplomatie » (McLaughlin, 2005). Le chapeautage gouvernemental de l'ISC est un bon exemple de ce type de diplomatie.

Il est également important de noter que les mesures de contrôle d'Internet dans les régimes autoritaires sont moins susceptibles d'être en phase avec les avancées technologiques qu'ailleurs. En d'autres termes, lorsqu'un régime autoritaire parvient à construire une nouvelle souricière, les compagnies technologiques fabriquent de meilleures souris. De nombreux exemples viennent renforcer cette affirmation. Par exemple, au sein de plusieurs régimes autoritaires, des fournisseurs Internet illégaux donnent accès aux sites bloqués dans des cybercafés, universités et résidences privées. Ils exploitent généralement les lacunes technologiques afin de contourner les filtres gouvernementaux et de charger des frais pour l'accès (Palmer, 2005). Un autre exemple est celui du Vietnam où des militants utilisent généreusement la voix sur IP (VoIP) pour entrer en contact, participer à des conférences téléphoniques et à débats en ligne et pour envoyer des messages vocaux enregistrés sur des forums Internet de certains sites qui utilisent le VoIP, comme PalTalk, Yahoo! Messenger et Skype (Johnson, 2006). En effet, la façon dont le protocole VoIP convertit les conversations en unités numériques rend difficile le filtrage des mots inadéquats en comparaison, par exemple, à des courriels.

Comme la Chine le démontre, les régimes autoritaires ont donc besoin de l'aide des multinationales des pays développés. Dans le cas chinois, de nombreuses multinationales étrangères coopèrent avec le gouvernement en échange d'un accès à son gigantesque marché du commerce électronique.

Les réponses des compagnies de technologies

Le pouvoir d'influencer l'évolution d'une organisation varie selon l'acteur institutionnel. Le gouvernement chinois, par exemple, peut s'attendre à exercer un plus grand contrôle sur les compagnies de technologies basées en Chine. Beau-

coup d'entrepreneurs chinois revenant d'Occident satisfont les demandes du gouvernement pour fournir la technologie de filtrage de la cyberpolice. Les compagnies de technologie occidentales, toutefois, sont tenues de rassurer différentes organisations concurrentes. Elles doivent ainsi décupler leurs réponses.

La nature exacte du découplage dépend de la perception des pouvoirs relatifs d'organisations concurrentes et des intérêts institutionnels (March et Olsen, 1989). Ces études étayent également la notion selon laquelle les réponses substantielles ne peuvent pas être faites pour rassurer des acteurs qui sont diamétralement opposés. Dit plus simplement, la réponse foncière a trait à la menace ou à l'occasion associées à l'acteur qui est perçu comme étant le plus puissant, et la réponse symbolique a trait à la menace ou à l'occasion associées à l'acteur qui est perçu comme possédant moins de pouvoir (George et autres, 2006).

À cet effet, selon l'e-Business Research Center de Chine et le CNZZ Data Center, le marché chinois du commerce électronique a atteint 703 milliards de dollars en 2010, soit une augmentation de 22 % par rapport à 2009 (Lan, 2011). Le gouvernement chinois possède donc un pouvoir énorme sur ces multinationales. Pour avoir accès au gigantesque marché du commerce électronique de la Chine, les compagnies occidentales semblent être prêtes à entreprendre des actions qui ne sont pas conformes à celles ayant cours dans leur pays d'origine.

Le gouvernement chinois a mis sur pied la « grande muraille pare-feu de Chine » avec l'aide de compagnies étrangères telles que Cisco Systems (Gutmann, 2002). Cisco a également muni la Chine d'équipements pour assister la cyberpolice chinoise dans ses activités de surveillance des communications électroniques (Jasper, 2006). Environ le quart des exposants au Salon de la sécurité 2000 en Chine, pour la plupart des sociétés étrangères, faisaient la promotion de produits destinés à renforcer le « Bouclier d'or » de la Chine (Fackler, 2000). En résumé, plusieurs entreprises spécialisées en technologies occidentales ont choisi de coopérer avec le gouvernement chinois.

Les décideurs organisationnels peuvent avoir une perception dissemblable des pouvoirs relatifs qu'ont les différents intérêts organisationnels et institutionnels. De la même façon, leurs réponses aux pressions vont varier. Parmi les entreprises de technologies étrangères, la stratégie adoptée par Yahoo! peut être décrite comme une stratégie de complaisance : « une obéissance consciente aux valeurs, normes ou exigences institutionnelles, ou l'intégration de celles-ci » (Oliver, 1991, p. 152). Le patron de Yahoo!, Jerry Yang, a affirmé qu'il devait prendre la décision d'aider les autorités chinoises à arrêter un journaliste pour obtenir le droit de faire des affaires en Chine (McLaughlin, 2005). En revanche, on peut avancer que contrairement à de nombreuses entreprises chinoises spécialisées en technologies, qui peuvent avoir inconsciemment adhéré aux règles locales (Oliver, 1991, p. 199), la stratégie de complaisance d'entreprises de technologies étrangères comme Yahoo! est consciemment et stratégiquement choisie afin de se conformer aux pressions institutionnelles en vue d'en tirer des bénéfices dans leur propre intérêt, ou d'avoir accès aux ressources.

Au début des années 2000, d'autres compagnies étrangères, tels Google et AltaVista, ont répondu différemment. La réponse de ces entreprises aux pressions

institutionnelles relatives au cybercontrôle en Chine peut être décrite comme de « l'évitement » (Meyer et Rowan, 1977). Une telle stratégie peut également en être une de « fuite », qui suppose de quitter « le champ au sein duquel la pression est exercée » (Oliver, 1991, p. 155).

Les réponses de Yahoo!, Google et AltaVista ne sont pas socialement acceptables dans leur pays d'origine. La perspective de ne pas avoir accès aux ressources motive les chefs d'entreprise à trouver des solutions de rechange qui peuvent exister au-delà des frontières de l'acceptabilité sociale (March et Simon, 1958). Les théoriciens soutiennent que ces entreprises auront tendance à perdre l'accès aux ressources si elles adhèrent aux pratiques courantes. Pour cette raison, elles peuvent sous-évaluer les risques associés au fait d'abandonner des façons de faire établies et de remettre en question la légitimité de ces pratiques et, par conséquent, elles tenteront d'établir une structure encadrant les nouvelles façons de faire par des changements non isomorphes (George et autres, 2006).

■ CONCLUSION

La discussion qui suit fournit des pistes pour comprendre les processus institutionnels associés au contrôle d'Internet dans les régimes autoritaires. Les découvertes faites sont largement conséquentes avec les théories existantes sur la formation des champs. Néanmoins, cet article a révélé des structures et des mécanismes associés aux mesures de contrôle d'Internet en Chine.

S'il y a une leçon à retenir des vastes actions d'espionnage électronique menées récemment, c'est que les pays ayant de grandes capacités en matière d'espionnage électronique et de cyberguerre comme la Chine seront en bonne position pour exploiter les faiblesses du « nuage » afin de mener de telles activités. Dans le cas du Shadow Network, le réseau d'espionnage électronique combinait les réseaux sociaux et les plateformes infonuagiques, dont celles de Google, Baidu, Yahoo!, Twitter, Blogspot et blog.com, ainsi que les serveurs traditionnels de commandement et contrôle (Information Warfare Monitor/Shadowserver Foundation, 2010).

De nombreux aspects de l'environnement institutionnel peuvent affaiblir la valeur de l'offre de l'infonuagique et décourager les investisseurs. En 2008, le P.-D.G. de Google a annoncé que sa compagnie allait travailler de concert avec les universités chinoises, à commencer par l'Université de Tsinghua, sur des programmes universitaires portant sur l'infonuagique. Le cyberenvironnement chinois, défavorable du point de vue de la sécurité, toutefois, a mené au retrait de Google de la Chine. À ce sujet, les fournisseurs de technologies nuagières basés en Chine pourront rencontrer des obstacles à l'internationalisation de leurs activités, surtout parce que la sécurité est parmi les préoccupations principales en matière d'homologation de « nuages ». Une de ces préoccupations est que l'environnement institutionnel de la Chine ne peut pas garantir la sécurité et la protection des données des usagers. À cause de la réputation du gouvernement chinois, on craint que les données stockées dans un « nuage » hébergé en Chine ne soient pas en sécurité. Ces préoccupations deviennent plus importantes encore lorsque nous envisageons la possibilité que le gouvernement contrôle les fournisseurs de technologies nuagières basés en Chine.

BIBLIOGRAPHIE

Aldrich, M. (1999). *E-Com Legal Guide: China, Baker and McKenzie*, Hong Kong, www.bakerinfo.com/apec/chinaapec.htm (page consultée le 11 décembre 2006).

Asia Pulse (2006). *China's Online Transactions Seen to Reach US$125*, www.bushwatch.com/archive2006/e-mail-20060719.htm (page consultée le 30 avril 2007).

Backoff, J. F. et C. L. Martin Jr. (1991). « Historical Perspectives: Development of the Codes of Ethics in the Legal, Medical and Accounting Professions », *Journal of Business Ethics*, vol. 10, n° 2, p. 99-110.

Basu, O., M. Dirsmith et P. Gupta (1999). « The Coupling of the Symbolic and the Technical in an Institutionalized Context: The Negotiated Order of the GAO's Audit Reporting Process », *American Sociological Review*, vol. 64, p. 506-526.

BBC News (2002a). *China Blocking Google*, http://news.bbc.co.uk/1/hi/technology/2231101.stm (page consultée le 28 janvier 2008).

BBC News (2002b). *Google Fights Chinese Ban*, http://news.bbc.co.uk/1/hi/technology/2233229.stm (page consultée le 28 janvier 2008).

Bremmer, I. (2006). « The World is J-curved », Washington Post, 1er octobre, p. B.3.

Brint, S. et J. Karabel (1991). « Institutional Origins and Transformations: The Case of American Community Colleges », dans W. Powell et P. DiMaggio (dir.), *The New Institutionalism in Organizational Analysis, Chicago*, University of Chicago Press, p. 337-360.

Burt, R. S. (1983). *Corporate Profits and Cooptation: Networks of Market Constraints and Directorate Ties in the American Economy*, New York, Academic Press.

Camenisch, P. E. (1983). *Grounding Professional Ethics in a Pluralistic Society*, New York, Haven Publications.

Campbell, J. L. (2004). *Institutional Change and Globalization*, Princeton, Princeton University Press.

Christensen, T. (1996). « Chinese Realpolitik », *Foreign Affairs*, vol. 75, n° 5, p. 37-52.

Claypool, G. A., D. F. Fetyko et M. A. Pearson (1990). « Reactions to Ethical Dilemmas: A Study Pertaining to Certified Public Accountants », *Journal of Business Ethics*, vol. 9, n° 9, p. 699-706.

Clemens, E. S. et J. M. Cook (1999). « Politics and Institutionalism: Explaining Durability and Change », *Annual Review of Sociology*, vol. 25, p. 441-466.

Crampton, T. (2006). « Innovation may Lower Net Users' Privacy. Embraced by China, New Standard Helps to Trace People Online », *International Herald Tribune*, 20 mars, p. 1.

DiMaggio, P. J. (1988). « Interest and Agency in Institutional Theory », dans L. Zucker (dir.), *Institutional Patterns and Organizations*, Cambridge, Ballinger, p. 3-22.

E-Commerce Times (2008). *China Dismantles 44,000 Sites in Anti-porn Offensive*, www.ecommercetimes.com/story/China-Dismantles-44000-Sites-in-Anti-Porn-Offensive-61336.html?welcome=1201374030 (page consultée le 28 janvier 2008).

Economist (2002). « Asia: Stop your Searching. The Internet in China », *Economist*, 7 septembre, p. 68.

Einhorn, B. (2008). *New Regulations for China's YouTube Wannabes*, www.macnewsworld.com/story/web20/61268.html (page consultée le 26 janvier 2008).

Einhorn, B., A. Webb et P. Engardio (2000). « China's Tangled Web », *Business Week*, 17 juillet, p. 56-58.

Elsbach, K. D. et R. I. Sutton (1992). « Acquiring Organizational Legitimacy through Illegitimate Actions: A Marriage of Institutional and Impression Management Theories », *Academy of Management Journal*, vol. 35, n° 4, p. 699-738.

Espiner, T. (2010). *Cable Reveals US Concerns over Chinese Cyber-Warfare*, www.zdnet.co.uk/news/security-threats/2010/12/06/cable-reveals-us-concerns-over-chinese-cyber-warfare-40091072/ (page consultée le 28 février 2012).

Fackler, M. (2000). *The Great Fire Wall of China?*, www.abcnews.go.com/secions/tech/DailyNews/chinanet001108.html (page consultée le 28 février 2012).

Foreign Policy (2011). *The FP Survey: The Internet*, septembre-octobre, 188, p. 1-9.

Foushee, H. (2006). « Gray Area: The Future of Chinese Internet », *Harvard International Review*, vol. 8, n° 2, p. 8-9.

Fowler, G. A. (2006). « Great Firewall: Chinese Censors of Internet Face "Hacktivists" in US ; Programs Like Freegate, Built by Expatriate Bill Xia, Keep the Web Worldwide ; Teenager Gets His Wikipedia », *Wall Street Journal*, 13 février, p. A.1.

French, H. W. (2006). « Chinese Discuss Plan to Tighten Restrictions on Cyberspace », *New York Times*, 4 juillet, p. A.3.

George, E. et autres (2006). « Cognitive Underpinnings of Institutional Persistence and Change: A Framing Perspective », *Academy of Management Review*, vol. 31, n° 2, p. 347-385.

Guillén, M. F. et S. L. Suárez (2005). « Explaining the Global Digital Divide: Economic, Political and Sociological Drivers of Cross-national Internet Use », *Social Forces*, vol. 84, n° 2, p. 681-708.

Guoguang, W. (2006). « The Peaceful Emergence of a Great Power ? », *Social Research*, vol. 73, n° 1, p. 317-345.

Gutmann, E. (2002). « Who Lost China's Internet? », *The Weekly Standard*, vol. 7, n° 23, 15 février, p. 24-29.

Hachigian, N. (2001). « China's Cyber-strategy », *Foreign Affairs*, vol. 80, n° 2, p. 118-133.

Hirsch, P. (1997). « Sociology without Social Structure: Neo-institutional Theory Meets Brave New World », *American Journal of Sociology*, vol. 102, n° 6, p. 1702-1723.

Hoffman, A. J. (1999). « Institutional Evolution and Change: Environmentalism and the US Chemical Industry », *Academy of Management Journal*, vol. 42, n° 4, p. 351-371.

Hvistendahl, M. (2010). *China's Hacker Army*, www.foreignpolicy.com/articles/2010/03/03/china_s_hacker_army ?page=full (page consultée le 28 février 2012).

Hvistendahl, M. (2009). « The China Syndrome », *Popular Science*, vol. 274, n° 5, p. 60-65.

Information Warfare Monitor et Shadowserver Foundation (2010). *Shadows in the Cloud: Investigating Cyber Espionage 2.0*, www.nartv.org/mirror/shadows-in-the-cloud.pdf (page consultée le 28 février 2012).

Jasper, W. F. (2006). « Terror in America, Made in China », *New American*, vol. 22, n° 6, p. 19-21.

Jesdanun, A. (2008). *China Catching up to US in Number of Web Surfers*, http://www.technewsworld.com/story/China-Catching-Up-to-US-in-Number-of-Web-Surfers-61292.html?welcome=1201370753 (page consultée le 26 janvier 2008).

Johnson, K. (2006). « Voices of Dissent », *Time International*, 25 septembre, p. 50.

Kahn, J. (2006). « China Says Web Controls Follow the West's Lead », *New York Times*, 15 février, p. A.6.

Kalathil, S. (2003). « China's New Media Sector: Keeping the State in », *Pacific Review*, vol. 16, n° 4, p. 489-501.

Keizer, G. (2010). *Chinese Firm Hired Blaster Hacking Group, Says U.S. Cable*, www.computerworld.com/s/article/9199898/Chinese_firm_hired_Blaster_hacking_group_says_U.S._cable (page consulté le 28 février 2012).

Kshetri, N. (2011). « Cloud Computing in the Global South: Drivers, Effects and Policy Measures », *Third World Quarterly*, vol. 32, n° 6, p. 995-1012.

Kshetri, N. (2010a). « Cloud Computing in Developing Economies », *IEEE Computer*, vol. 43, n° 10, p. 47-55.

Kshetri, N. (2010b). *The Global Cyber-crime Industry: Economic, Institutional and Strategic Perspectives*, New York, Springer-Verlag.

Kshetri, N. (2007). « The Adoption of e-Business by Organizations in China: An Institutional Perspective », *Electronic Markets*, vol. 17, n° 2, p. 113-125.

Kshetri, N. et M. K. Cheung (2002). « What Factors are Driving China's Mobile Diffusion ? » *Electronic Markets*, vol. 12, n° 1, p. 22-26.

Kshetri, N. et N. Dholakia (2001). *Impact of Cultural and Political Factors on the Adoption of Digital Signatures in Asia*, Communication présentée à l'Americas' Conference on Information Systems, Boston, 3-5 août.

Kshetri, N., N. Dholakia et A. Awasthi (2003). *Determinants of e-Government Readiness: Evidence from China and India*, Communication présentée au First International Conference on e-Governance, New Delhi, 18-20 décembre.

Kshetri, N., P. Palvia et H. Dai (2011). « Chinese Institutions and Standardization: The Case of Government Support to Domestic Third Generation Cellular Standard », *Telecommunications Policy*, vol. 35, n° 5, p. 399-412.

Lan, T. (2011). « Real Rules for Virtual Space », *Beijing Review*, vol. 54, n° 47, p. 12-13

Li, M., Z. Lin et M. Xia (2004). « Leveraging the Open Source Software Movement for Development of China's Software Industry », *Information Technologies and International Development*, vol. 2, n° 2, p. 45-63.

Los Angeles Times (1997). « The Cutting Edge ; Testing the Boundaries ; Countries Face Cyber Control in their Own Ways », *Los Angeles Times*, 30 juin, p. 1.

MacKinnon, R. (2012). *Inside China's Censorship Machine*, http://fullcomment.nationalpost.com/2012/01/29/rebecca-mackinnon-inside-chinas-censorship-machine/ (page consultée le 22 février 2012).

Mallaby. S. (2006). « Google and my Red Flag », *The Washington Post*, 30 janvier, p. A.17.

March, J. G. et J. P. Olsen (1989). *Rediscovering Institutions: The Organizational Basis of Politics*, New York, Free Press.

March, J. G. et H. Simon (1958). *Organizations*, New York, Wiley.

Marsh, C. et J. T. Dreyer (2003). *US-China Relations in the Twenty-First Century: Policies, Prospects, and Possibilities*, Lanham, Lexington Books.

McLaughlin, K. E. (2005). « China's Model for a Censored Internet », *Christian Science Monitor*, vol. 97, p. 1-10.

McMillan, R. (2010). *More Than 100 Companies Targeted by Google Hackers*, www.computerworld.com/s/article/9163158/More_than_100_companies_targeted_by_Google_hackers (page consultée le 28 février 2012).

Meyer, J. et B. Rowan (1977). « Institutionalized Organizations: Formal Structure as Myth and Ceremony », *American Journal of Sociology*, vol. 83, n° 2, p. 333-363.

Meyer, J. W., W. R. Scott et T. E. Deal (1983). « Institutional and Technical Sources of Organizational Structure: Explaining the Structure of Educational Organizations », dans J. W. Meyer et W. R. Scott (dir.), *Organizational Environments*, Beverly Hills, Sage, p. 45-67.

Myers, W. H. (1996). « The Emerging Threat of Transnational Organized Crime from the East », *Crime, Law and Social Change*, vol. 24, n° 3, p. 181-222.

Oliver, C. (1991). « Strategic Responses to Institutional Processes », *Academy of Management Review*, vol. 16, n° 1, p. 145-179.

Palmer, K. (2005). « Contrabandwidth », *Foreign Policy*, vol. 147, mars-avril, p. 93.

Pei, M. (2006). « The Dark Side of China's Rise », *Foreign Policy*, vol. 153, mars-avril, p. 32-40.

Pei, M. (2003). « The Paradoxes of American Nationalism », *Foreign Policy*, vol. 13, mai-juin, p. 30-37.

Popov, V. (2006). « Foreign Direct Investment in Russia: Why Doesn't It Come? Should There Be More of It? », *Canadian Foreign Policy*, vol. 13, n° 2, p. 51-64.

Precision Marketing (2003). *Mobile Industry to Clamp Down on Youth Marketing*, 12 décembre, p. 3.

Rodan, G. (1998). « The Internet and Political Control in Singapore », *Political Science Quarterly*, vol. 113, n° 1, p. 63-99.

Russell, J. (2011). *China to Develop $154m Tech Centre Free of Web Restrictions*, www.asiancorrespondent.com/58249/china-to-develop-154m-tech-centre-free-of-web-restrictions/ (page consultée le 22 février 2012).

Sautman, B. (2001). « Peking Man and the Politics of Paleoanthropological Nationalism in China », *Journal of Asian Studies*, vol. 60, n° 1, p. 95-124.

Scott, W. R. (2001). *Institutions and Organizations*, 2e édition, Thousand Oaks, Sage.

Scott, W. R. (1995). *Institutions and Organizations*, Thousand Oaks, Sage.

Shen, X. (2005). « A Dilemma for Developing Countries in Intellectual Property Strategy? Lessons from a Case Study of Software Piracy and Microsoft in China », *Science and Public Policy*, vol. 32, n° 3, p. 187-198.

Shie, T. R. (2004). « The Tangled Web: Does the Internet Offer Promise or Peril for the Chinese Communist Party? », *Journal of Contemporary China*, vol. 13, n° 40, p. 523-540.

Singer, M. (2002). *Google Blocked in China*, http://siliconvalley.internet.com/news/article.php/1455921 (page consultée le 11 décembre 2003).

Stevenson-Yang, A. (2006). « China's Online Mobs: The New Red Guard? », *Far Eastern Economic Review*, vol. 169, n° 8, p. 53-57.

Stoner-Weiss, K. (2006). « Russia: Authoritarianism without Authority », *Journal of Democracy*, vol. 17, n° 1, p. 104-118.

Stout, K. L. (2002). *China Sites Count Cost of Cyber-control*, www.cnn.com/2002/TECH/11/03/china.content/ (page consultée le 11 décembre 2006).

Su, F. et D. L. Yang (2000). « Political Institutions, Provincial Interests, and Resource Allocation in Reformist China », *Journal of Contemporary China*, vol. 9, n° 24, p. 215-230.

Terrill, R. (2005). « What does China Want ? », *Wilson Quarterly*, vol. 29, n° 4, p. 50-61.

Tolbert, P. S. et L. G. Zucker (1996). « The Institutionalization of Institutional Theory », dans S. R. Clegg, C. Hardy et W. R. Nord (dir.), *Handbook of Organization Studies*, London, Sage, p. 175-190.

US Fed News Service, Including US State News (2006). *Human Rights: Somalia, Mauritania and the Internet*, www.europarl.europa.eu/news/expert/infopress_page/015-9503-187-07-28-902-20060629IPR09390-06-07-2006-2006-false/default_de.htm (page consultée le 30 avril 2008).

Wang, L. (2011). *China Seeks to Work with Taiwan in Smart Devices and Cloud Computing*, www.taipeitimes.com/News/biz/archives/2011/06/18/2003506036 (page consultée le 22 février 2012).

Ward, S. P. et autres (1993). « Certified Public Accountants: Ethical Perceptions, Skills and Attitudes on Ethics Education », *Journal of Business Ethics*, n° 12, p. 601-610.

Weaver, L. R. (2002). *Report: China Blocks Another Search Engine*, www.edition.cnn.com/2002/TECH/internet/09/06/china.internet.block/index.html (page consultée le 28 janvier 2008).

West, D. M. (2002). *Global e-Government, 2002*, www.insidepolitics.org/egovt02int.PDF (page consultée le 22 juin 2003).

White, H. (1992). *Identity and Control: A Structural Theory of Social Interaction*, Princeton, Princeton University Press.

Wilson III, E. J. et A. Segal (2005). « Trends in China's Transition Toward a Knowledge Economy », *Asian Survey*, vol. 45, n° 6, p. 886-906.

Yang, D. L. (2001). « The Great Net of China », *Harvard International Review*, vol. 22, n° 4, p. 64-69.

Zhang, X. et V. R. Prybutok (2005). « How the Mobile Communication Markets Differ in China, the U.S., and Europe », *Communications of the ACM*, vol. 48, n° 3, p. 111-144.

Zittrain, J. (2009) « Lost in the Cloud », *nytimes.com*, www.nytimes.com/2009/07/20/opinion/20zittrain.html ?bl&ex=1248235200&en=7d30b8c05442733a&ei=5087%0A (page consultée le 1er décembre 2009).