diploweb.com La revue géopolitique
ISSN : 2111-4307

Chine : cyberstratégie, l’art de la guerre revisité

jeudi 12 septembre 2013,par Frédérick DOUZET

Citer cet article / To cite this version :
Frédérick DOUZET, **Chine : cyberstratégie, l’art de la guerre revisité** , *Diploweb.com : la revue géopolitique, 12 septembre 2013.*

La Chine est devenue un acteur majeur et incontournable du cyberespace, avec une volonté claire d'exister, de développer ses outils stratégiques et de ne pas dépendre technologiquement d'autres nations pour maîtriser au mieux l'information stratégique. Bien que le régime ait développé d'importantes cybercapacités, elles semblent moins centralisées, coordonnées et maîtrisées que ce que les discours sur la menace chinoise laissent à croire. Dans le brouillard juridico-stratégique du cyberespace, la Chine pousse cependant son avantage en menant des offensives de basse intensité et une politique de renseignement et d'influence qui témoigne de sa volonté de fomenter les outils de sa puissance et de se positionner comme un acteur avec lequel il faudra compter.

Le *Diploweb.com* est heureux de vous présenter cet article inédit dans le cadre de son partenariat avec le 24ème Festival International de Géographie : "La Chine, une puissance mondiale", 3 au 6 octobre 2013, Saint-Dié-des-Vosges.

A L'HEURE où les grandes puissances occidentales multiplient les initiatives et les investissements pour développer une stratégie cohérente face aux cybermenaces, la Chine fait paradoxalement figure de *leader.* Sa capacité à intégrer la dimension cyber dans tous les domaines stratégiques de sa montée en puissance - aussi bien militaire, que politique ou économique - impressionne, inquiète et suscite en réaction de vifs débats qui révèlent les contradictions et les fragmentations de la réflexion stratégique occidentale, dans un contexte de tensions géopolitiques qui rappelle le temps de la guerre froide.

Partie tardivement dans la course au développement de l'Internet, la Chine a en effet compensé son handicap technologique par le développement rapide d'une stratégie compréhensive qui s'appuie sur les principes de l'art ancestral de la guerre, notamment la volonté de développer une supériorité informationnelle aussi bien offensive que défensive.

L'élaboration de la cyberstratégie de la Chine

Sur le plan intérieur, le régime s'est montré particulièrement créatif en matière de censure et de propagande, usant d'un savant alliage de technologie de pointe, de pratiques éprouvées d'oppression politique (intimidation, collaboration forcée, délation, surveillance, répression), d'un arsenal juridique et d'offensives de communication pour museler l'opposition collective et contrôler le contenu.

L'impératif de survie du régime autoritaire a stimulé la réflexion stratégique des dirigeants en la matière. D'entrée, le gouvernement a pris le contrôle de la distribution de la connectivité et par la force d'attractivité de sa croissance économique, a contraint les entreprises américaines à développer la technologie de filtrage permettant de contrôler l'information en circulation, construisant ainsi une véritable muraille du Net autour du pays. La Chine s'est dotée d'une patrouille de l'Internet, a contraint les fournisseurs d'accès à fournir les coordonnées des utilisateurs, a fermé des cybercafés dans l'irrégularité par centaines et s'est donné les moyens de couper ou ralentir le trafic vers les serveurs politiquement incorrects, dont le célèbre Google.

Aussi sophistiquée soient-elles, les méthodes n'ont pas résisté à la croissance exponentielle du

nombre d'utilisateurs, passé de 137 à 538 millions en 6 ans. Mais là encore le régime n'a cessé de s'adapter. Une étude récente [1] montre que désormais, la stratégie de censure ne vise plus à empêcher l'opposition de critiquer le parti et ses dirigeants, y compris de façon virulente, mais à l'empêcher de s'organiser collectivement**. Le régime est ainsi capable de trouver, analyser et tout simplement supprimer de l'Internet les propos qui représentent, renforcent ou encouragent la mobilisation sociale**. Sa cohésion interne est aussi un enjeu pour son existence sur la scène internationale. Elle a également su soumettre les acteurs internationaux (notamment américains) à ses velléités de contrôle. On se souvient du bras de fer avec Google en 2010 suite à des intrusions répétées sur des messageries *Gmail* de dissidents chinois.

Face à la supériorité militaire des Etats-Unis, le régime a choisi l'approche asymétrique, menant une offensive tous azimuts visant à exploiter toutes les ressources du cyberespace, dans une optique de modernisation de son armée. Elle vise à recueillir, par des voies légales ou illégales, de l'information de haut niveau scientifique, technologique, économique mais aussi politique et stratégique (veille, intelligence, intrusions, espionnage).

Le maître mot est « informationisation », **une conception stratégique de l'information qui se trouve désormais au cœur de tous les supports de l'expression de la puissance chinoise**. La maîtrise de l'information est devenue prioritaire et indissociable de tous les autres domaines, aussi bien militaires que politiques ou économiques. Avoir la capacité de recueillir par de multiples sources, recouper, vérifier l'information pour s'assurer de sa fiabilité, mais aussi de la manipuler, la déformer, la transformer pour tromper ou faire douter l'adversaire, autant de **techniques ancestrales qui avec l'interconnexion croissante des réseaux et la rapidité de circulation de l'information des prennent des proportions inédites**. Les opérations sur les réseaux d'information et de communication sont désormais indissociables de tout conflit et de toute opération militaire. Cette stratégie explicitée dans l'ouvrage *Unrestricted Warfare* (*la guerre sans limite*) de deux anciens colonels de l'Armée de Libération Populaire, Qiao Liang and Wang Xiangsui, publié en anglais en 1999, a renforcé les inquiétudes sur les cybercapacités de la Chine.

La montée en puissance internationale

La Chine s'affirme aussi au niveau international par son lobbying sur la gouvernance de l'Internet, sa tentative d'autonomisation du réseau, le renforcement de sa zone d'influence et ses démonstrations de force. Comme en Russie, le gouvernement considère son réseau comme un domaine de souveraineté qui doit relever de son contrôle, une position totalement à l'opposée des Etats-Unis qui défendent un Internet libre et ouvert, gouverné par un organe indépendant mais néanmoins sous tutelle du secrétariat du commerce américain.

En 2010, la Chine est accusée d'avoir détourné 15% du trafic internet mondial (« hijacking ») pendant 18 minutes, une façon de laisser entrevoir ses capacités sans pour autant que le gouvernement reconnaisse la moindre implication. En matière de cyber, la question de l'attribution (qui est réellement derrière une attaque et pourquoi) reste entière et la Chine proteste vivement contre les accusations d'espionnage visant le gouvernement ou l'armée, estimant que les Etats-Unis sont largement supérieurs d'un point de vue technologique et que la Chine est la première victime des attaques.

Elle développe enfin **une politique industrielle qui la place au cœur du système**, avec la fabrication à des coûts défiant toute concurrence d'équipements, notamment de routeurs, matériels très utiles pour qui veut observer le trafic Internet. La Chine a lancé des satellites de navigation auquel ironiquement la NSA a continué à avoir recours, en pleine escalade des tensions sur le cyberespionnage, alors que le Congrès dans une résolution budgétaire interdisait l'utilisation de matériel informatique chinois par le gouvernement et la défense.

A l'égard des grandes puissances mais aussi des puissances régionales de l'ASEAN, la Chine est accusée de multiplier les attaques de faible impact (intrusions sans dommages dans les réseaux), dont l'intensité n'est pas suffisante pour déclencher un conflit ouvert mais qui sont autant de messages sur les cybercapacités du pays et d'outils stratégiques. Les intrusions dans les systèmes permettent non seulement de recueillir des informations cruciales mais aussi de cartographier les vulnérabilités des réseaux ou de constituer des armées de zombies (ordinateurs infectés par un virus mobilisables pour une attaque) qui pourront être exploitées dans d'autres circonstances, en cas de crise.

Du point de vue américain et européen, la cyberstratégie chinoise est souvent présentée comme coordonnée et centralisée au plus haut niveau de gouvernement et commandement militaire, et dotée d'une efficacité redoutable. Pour autant, si le gouvernement a su faire preuve d'ingéniosité et d'adaptabilité, force est de constater que nombre d'initiatives échappent à son contrôle. De jeunes hackers chinois rivalisent d'audace pour assurer leur carrière ou affirmer la puissance de leur employeur (entreprise, agence d'Etat ou civils indépendants…), bien souvent hors de la supervision de stratèges séniors, dépassés par la technique. Les attaques se multiplient au sein même de la Chine, avec des conséquences préoccupantes pour l'économie. Les discussions diplomatiques montrent l'émergence de réelles préoccupations et la recherche d'une stratégie plus centralisée, d'une possible coopération internationale sur l'établissement de règles communes et contre la prolifération des cyberarmes, ce que les Russes dénoncent comme la militarisation du cyberespace.

La cybermenace chinoise : une invention américaine ?

Alors, la cybermenace chinoise serait-elle exagérée ? Depuis le début de l'année 2013, on assiste à une véritable montée en puissance du discours sur la menace chinoise et une escalade des tensions entre les Etats-Unis et la Chine. Révélations dans la presse sur les cyberattaques chinoises, sortie du rapport Mandiant à la veille de la plus importante conférence sur la sécurité informatique aux Etats-Unis, accusations de plus en plus directe de l'administration Obama contre le gouvernement chinois, fuite dans la presse d'un rapport juridique secret autorisant le président américain à des frappes pré-emptive pour contrer les cyberattaques… Après avoir sommé les fabricants chinois Huawei et ZTE de s'expliquer devant le Sénat sur la possible implantation de *backdoors* (portes dérobées) dans leurs équipements, permettant d'espionner les utilisateurs, les dirigeants américains ont expliqué au Congrès que **le risque cyber surpassait désormais le risque terroriste**.

L'affaire **PRISM** a révélé ce que nombre d'experts savaient déjà : **la Chine n'est pas le seul enfant terrible du cyberespace**, loin de là. Et toute la propagande chinoise est désormais axée sur l'affaire Snowden qui a révélé en juin 2013 **l'ampleur de la surveillance menée par la NSA aux Etats-Unis et dans le monde. La France, la Russie, Israël** sont également réputés pour leur utilisation offensive des cybercapacités. Toutes les attaques dont la trace

remonte en Chine ne proviennent pas nécessairement de Chine tant les serveurs sont relativement simples à pénétrer et peuvent faire écran aux desseins d'autres acteurs. Il n'est nullement question de nier l'ampleur des intrusions et de l'espionnage mené par la Chine mais de relativiser le discours que d'autres nations peuvent tenir à son encontre.

Les Chinois pointent à juste titre la très grande centralisation de la politique de cyberdéfense américaine (**US CYBERCOMMAND**), plutôt surprenante venant d'un Etat fédéral aussi décentralisé, et l'avalanche de moyens qui lui sont consacrés aux Etats-Unis. Le **Général Keith Alexander, directeur du cybercom mais également de la NSA**, affirme désormais clairement le développement de capacités offensives ainsi que l'augmentation considérable de ses effectifs et de son budget (+ $800 millions), en pleine période de restrictions budgétaires.

Les représentations de la menace chinoise ne sont pas nouvelles et montent en puissance depuis plusieurs années dans le discours stratégique américain, pour des raisons géopolitiques liées au contexte de rivalités internationales et domestiques. La perception de la menace repose sur le prémice d'une volonté hégémonique de la Chine, dont l'ascension économique, militaire et politique serait dangereuse en raison de sa volonté de puissance et d'expansion. C'est une vision partagée par les stratèges réalistes et pessimistes qui perçoivent les relations internationales comme un jeu à somme nulle, où l'ascension des uns conduirait nécessairement à la perte de puissance des autres. En l'occurrence, la Chine pourrait remettre en question la puissance d'une Amérique sur le déclin. Cette représentation repose aussi sur le présupposé que la Chine possède les moyens de ses ambitions, ce qui en matière cyber reste à démontrer. Les révélations sur les programmes de la NSA laissent à penser que **les Etats-Unis conservent une longueur d'avance**.

L'exacerbation de la cybermenace chinoise s'inscrit aussi dans un contexte politique interne aux Etats-Unis de véritable bras de fer entre l'administration Obama et le Congrès. Alors que leurs relations sont tombées dans l'impasse du *budget sequester*, elle permet de rappeler que les budgets fédéraux servent aussi au maintien de la sécurité nationale. Dans l'impossibilité de légiférer en raison d'une polarisation politique trop importante, l'administration Obama a joué le passage en force par décret présidentiel sur la cyberesécurité, en multipliant les alertes sur l'importance des enjeux.

Le discours de la menace est aussi porté par une multiplicité d'acteurs qui sont susceptibles d'y trouver leur intérêt, notamment financiers, alors que la cybersécurité fait partie des très rares budgets fédéraux en augmentation. Et **le marché florissant de la cybersécurité se porte d'autant mieux que la prise de conscience des risques est importante**.

Enfin, du point de vue de l'administration Obama, l'agitation de la menace chinoise pouvait aussi permettre de **détourner l'attention d'initiatives américaines qui pourraient être considérées comme « hors limites »**. Car à ce jour, la première attaque sérieuse qui pourrait être considérée comme un acte de « cyberguerre » reste le virus **Stuxnet**, élaboré par l'administration américaine en collaboration avec le gouvernement israélien pour perturber les programmes nucléaires iraniens, une sorte de troisième voie expérimentale entre la diplomatie coercitive et le conflit ouvert et dont les conséquences à venir restent à explorer.

Cette représentation de la menace chinoise, si on peut la relativiser, n'est pas pour autant anodine. Elle joue un rôle dans les rivalités de pouvoir géopolitique et pourrait conduire à une

escalade des tensions entre les Etats-Unis et la Chine, en dépit de l'interdépendance économique qui lie les deux puissances. Les révélations d'Edward Snowden ont fortement affaibli la position des Etats-Unis, aussi bien à l'égard de la Chine et de la communauté internationale qu'en interne. Il semble désormais impossible, dans le contexte de défiance publique actuelle, de pouvoir mettre en œuvre le plan de cyberdéfense qui jusqu'à récemment n'aurait suscité l'intérêt que d'une petite minorité d'initiés. Pour autant, la Chine semble chercher à sortir de la logique d'escalade pour discuter des règles de conduite dans le cyberespace en se posant comme une alternative à la position américaine. Une tentative dont il est bien trop tôt pour savoir ce qu'il en adviendra.

Conclusion

Une chose est claire, la Chine est devenue un acteur majeur et incontournable du cyberespace, avec une volonté claire d'exister, de développer ses outils stratégiques et de ne pas dépendre technologiquement d'autres nations pour maîtriser au mieux l'information stratégique. Bien que le régime ait développé d'importantes cybercapacités, elles semblent moins centralisées, coordonnées et maîtrisées que ce que les discours sur la menace chinoise laissent à croire. Dans le brouillard juridico-stratégique du cyberespace, la Chine pousse cependant son avantage en menant des offensives de basse intensité et une politique de renseignement et d'influence qui témoigne de sa volonté de fomenter les outils de sa puissance et de se positionner comme un acteur avec lequel il faudra compter.

Plus

. Le site du Festival International de Géographie : "La Chine, une puissance mondiale", 3 au 6 octobre 2013 à Saint-Dié-des-Vosges.

. Voir sur le *Diploweb.com* tous les articles et toutes les cartes sur la Chine.

Bibliographie

Séverine Arsène, 2011, *Internet et politique en Chine*, Karthala, Paris, 420 p.

Frédérick Douzet, « Les frontières chinoises de l'Internet », *Hérodote*, n°125, 2007.

Miguel Alberto N. Gomez, « Awaken the Cyber Dragon : China's Cyberstrategy and the Impact on ASEAN », International Conference on Cybersecurity, Cyber Peacefare and Digital Forensic (CyberSec2013).

Qiao Liang, Wang Xiangsui, *Unrestricted Warfare : China's Master Plan to Destroy America*, Pan American Publishing Company, 2002 (original edition : Beijing : PLA Literature and Arts Publishing House, February 1999).

Gary Ping, Jennifer Pan, Margaret E. Roberts, « How Censorship in China Allows Government Criticism but Silences Collective Expression », APSA 2012 Annual Meeting Paper.

Jean-Loup Samaan, *La menace chinoise. Une invention du Pentagone ?*, Vendémiaire, 2012.

David Sanger, Confront and Conceal : Obama's Secret War and Surprising Use of American Power, Broadway Books, 2012.
Justin Vaïsse, *Barack Obama et sa politique étrangère (2004-2008)*, Odile Jacob, 2012.

Séverine Arsène, 2011, *Internet et politique en Chine*, Karthala, Paris, 420p.

P.-S.

Titulaire de la Chaire Castex de Cyberstratégie (avec le soutien de la fondation d'entreprise EADS), Professeure à l'Institut Français de Géopolitique de l'Université Paris 8.

Notes

[1] Gary Ping, Jennifer Pan, Margaret E. Roberts, « How Censorship in China Allows Government Criticism but Silences Collective Expression », APSA 2012 Annual Meeting Paper.