diploweb.com La revue géopolitique
ISSN : 2111-4307

Stratégie du cyberespace

mercredi 13 février 2013,par Olivier KEMPF

Citer cet article / To cite this version :
Olivier KEMPF, **Stratégie du cyberespace** , *Diploweb.com : la revue géopolitique, 13 février 2013.*

Une rupture stratégique, l'avènement du cyberespace ? Oui, répond Olivier Kempf, parce que le cyber est opaque et non létal. L'offensive redevient possible, avec un allongement du temps stratégique, contrairement à une idée répandue. Et une question : une guerre cyber peut-elle déborder en guerre classique ?

LE CYBERESPACE est un mot en vogue ce qui peut susciter une certaine défiance : s'agit-il encore d'un produit de publicitaires ? Pourtant, à écouter tous les responsables publics et privés expliquer qu'il constitue un des défis majeurs de notre époque, il faut s'interroger et aller au-delà de la circonspection initiale. Surtout quand on entend le préfixe « cyber » associé à des sujets de préoccupations plus traditionnels comme la sécurité ou la défense. En effet, le cyberespace est non seulement nouveau et prégnant, mais il emporte des aspects stratégiques importants. Pour le comprendre, l'étude des caractéristiques stratégiques de ce cyberespace précédera la description des opportunités qu'il présente pour les différents acteurs, qui vont utiliser de nouvelles règles stratégiques.

I. Caractéristiques stratégiques du cyberespace

La première caractéristique du cyberspace est son universalité : non seulement le cyber [1] est désormais à la surface du globe, mais il est également présent dans tous les aspects de nos vies. Le phénomène s'observe dans des sociétés autrefois désignées sous le nom de « pays en voie de développement », qui entrent dans la bulle cyber grâce à la mise en place extrêmement rapide des réseaux de téléphonie sans fil. Mais le mouvement est encore plus patent dans les sociétés développées, où la couverture cybernétique est beaucoup plus épaisse. En effet, on ne saurait réduire le cyberespace à Internet, puisque tous les réseaux interconnectés, publics ou privés et quelque soit le moyen de leur interconnexion (fils, fibres, ondes de proximité, ondes satellites) participent du cyberespace. Ainsi, les ordinateurs en font bien sûr partie, mais il faut aussi inclure tous les ordiphones ou les réseaux privés de toute sorte (ceux des distributeurs automatiques de billet, ceux de la carte Vitale ou d'un laissez-passer Navigo). Ces différents réseaux coexistent, s'hybrident et pour certains s'isolent, mais ils tissent tous ensemble une couche « cyberspatiale » qui organise désormais nos vies. Comme pour l'électricité ou l'automobile, on ne pourra plus revenir en arrière.

Constatons de plus que ce nouvel espace ne peut être réduit à l'informatique. On peut le décrire selon un modèle en trois couches : une couche matérielle (car malgré l'apparence de « virtualité », le cyberespace repose sur une infrastructure physique extrêmement dense et souvent inaperçue) ; une couche logique (l'informatique proprement dite) ; et une couche sémantique, souvent omise, mais importante. On ne peut considérer la « donnée transportée « par les tuyaux » comme quelque chose de neutre : la donnée est « qualifiée », elle est information et ce qui est dit et la façon dont c'est dit font partie intégrante du cyberespace.

Le cyberespace est nouveau : ce truisme signifie qu'il est anthropogène et artificiel : il est donc profondément humain, ce qui justifie l'inclusion de sa dimension sociale dans l'analyse stratégique.

Cet espace social présente de plus la caractéristique d'inclure un nombre croissant d'acteurs. Stratégiquement, il ne peut être réduit à l'acteur traditionnel de la puissance qu'est l'Etat. Au contraire, le cyberespace inclut, pour la première fois de l'histoire, l'individu comme acteur

stratégique. L'individu est extrêmement mobile, il peut s'associer temporairement ou durablement, nouer des coalitions de circonstance ou s'associer à des projets très structurés et obtenir des effets « réels », dans le cyberespace ou grâce à lui.

Enfin, à considérer les intentions stratégiques des acteurs, on peut remarquer que le cyberespace présente deux dernières caractéristiques essentielles, qui vont orienter tous les calculs. Il s'agit tout d'abord du principe d'inattribution. L'opinion commune considère couramment que le cyberespace est celui de la transparence absolue, de l'accès immédiat à toutes les données. Or, les spécialistes peuvent aisément mener des actions cachées. Le cyberespace, malgré les apparences, est un espace opaque où l'on ne peut dresser le lien entre telle action et son auteur. Autrement dit, on ne peut « imputer » une attaque. Or, ne pas identifier l'adversaire constitue à la fois un immense avantage, et une immense difficulté. **Cet anonymat de la belligérance est stratégiquement nouveau**.

La deuxième caractéristique du cyberespace tient à sa **non-létalité** : les actions les plus conflictuelles ne sont pas létales (aujourd'hui du moins). Or, un des critères traditionnels de la guerre tient au fait de donner (ou recevoir) la mort. La non-létalité du cyberespace fait que les actions qui s'y mènent font peu de bruit, et surtout ne mobilisent pas aisément l'émotion médiatique. Voici la deuxième opacité du cyberespace, qui est en fait la conséquence de la première.

II. Opportunités stratégiques

Compte-tenu de ces caractéristiques, quelles vont être les attitudes stratégiques possibles ?

La première conséquence de l'opacité est le renouveau de la liberté de manœuvre des différents acteurs. Nous vivions dans un monde stratégique marqué par la défensive, pour plusieurs raisons : morale (surtout après les catastrophes des deux guerres mondiales), juridique (selon la charte des Nations-Unies, la seule cause légitime de guerre est la légitime défense), enfin et surtout technique, à cause de la domination de l'arme nucléaire. Celle-ci a en effet opéré un bouleversement stratégique qui a interdit la montée aux extrêmes. Toute guerre envisage, en effet, l'escalade de la violence, comme l'a très tôt montré Carl von Clausewitz. Avec le nucléaire, cette escalade devenait trop dangereuse : l'un des extrêmes apparaissait tellement fatal que personne ne prenait le risque d'ouvrir la montrée en entrant dans l'autre extrême, celui du déclenchement de la guerre puisque celle-ci pouvait naturellement croître jusqu'au conflit nucléaire. Ainsi, contrairement à une opinion couramment répandue, la stratégie nucléaire n'est pas une stratégie offensive, mais une stratégie fondamentalement défensive.

L'avènement du cyberespace (lui aussi fait technologique qui vient modifier la grammaire de la guerre) **provoque une nouvelle rupture stratégique. Puisqu'il est opaque, puisqu'il est non-létal, puisqu'on ne peut attribuer les actes à leurs auteurs, chacun peut « prendre l'initiative »**. Chacun, Etat, groupe ou individu, retrouve une liberté de manœuvre. En un mot, l'offensive redevient possible. Dès lors, les débats actuels sur son opportunité ne sont que de l'agitation médiatique : peu importe que les Etats-Unis ou Israël annoncent que leurs doctrines cyberstratégiques combinent défensive ou offensive, suivant en cela le discours précurseur et insuffisamment remarqué de la France qui, dès son *Livre Blanc* de 2008, annonçait son engagement dans cette direction : la nature stratégique du cyberespace,

ordonnée par le principe de l'inattribution, favorise le retour de l'offensive.

Toutefois, **ce retour de l'offensive doit obéir à la contrainte de l'opacité**. Ceci explique la mise en place d'une stratégie fondamentalement indirecte : Liddell-Hart et Beaufre en ont rêvé, le cyber l'a rendu possible. Voici au fond la réponse technologique aux développements asymétriques de la guerre, aux contournements récemment observés : le cyber permet de contourner le contournement des autres. Au fond, le cyber permet une sorte de resymétrisation de la conflictualité, puisque tous les acteurs vont pouvoir y opérer.

Toutefois, il faut faire attention : on évoque parfois la capacité du hacker a infiltrer tous les systèmes informatiques. Cela a pu être le cas au cours des années 1980, mais depuis les systèmes de protection et de défense se sont durcis. On assiste ainsi à un effet de gamme, où les grands acteurs jouent dans la même division. Comme au football, si tout le monde joue le même jeu, il y a les pros qui jouent en Ligue 1 et les amateurs du dimanche : mêmes règles mais différence d'efficacité, en défense comme en attaque. Ainsi, on peut dire sans trop de risques de se tromper que les Etats-Unis, la Chine, la Russie, la France, l'Allemagne, le Royaume-Uni, Israël, l'Inde jouent en ligue 1 : et comme en ligue 1, il y a les équipes qui luttent pour le titre, d'autres de milieu de tableau, et d'autres enfin qui luttent pour éviter la relégation.

Une autre conséquence de cette opacité est **l'allongement du temps stratégique**. Là encore, il faut se garder de l'illusion couramment colportée de l'instantanéité du cyber. A bien y regarder, on s'aperçoit que **les actions dans le cyber nécessitent une préparation et une anticipation**, d'autant plus longue que la cible est durcie. L'opération *Olympic Games*, qui visait à mettre en place le virus *Stuxnet* au sein de la centrale nucléaire iranienne de Natanz, fut décidée en 2006 : le virus mit trois ans avant d'être fabriqué et introduit dans la centrale (par une complicité humaine) et il opéra (de façon cachée) pendant un an avant que les Iraniens ne se rendent compte des dégâts. Au total, l'opération a duré quatre ans ! En fait, tout se passe comme si l'opacité permettait aussi d'échapper à l'accélération du temps que nous vivons collectivement et qui est d'ailleurs rendue possible par le développement de ce même cyberespace !

Remarquons enfin, pour conclure ce tableau trop bref, que la cyberconflictualité est **duale** : s'il peut y avoir des conflits uniquement cyber (c'est l'exemple de *Stuxnet*), il faut constater que le cyber recoupe d'autres conflictualités : aussi bien les guerres classiques existantes (cas du raid israélien contre la Syrie en 2007, cas des réactions talibanes en Afghanistan) que les conflits politiques qui font la une de l'actualité. Ainsi, et même si les médias en parlent peu, les conflits cyber font en ce moment rage au Proche et au Moyen Orient, et recoupent toutes les lignes de conflit existantes : Israéliens contre Palestiniens, Arabes contre Persans contre Turcs, chiites contre sunnites, Syriens contre opposants, Frères musulmans contre démocrates …. Et cette guerre recoupe une autre conflictualité, celle de la guerre économique : ainsi, on attaque la bourse de Tel–Aviv, les banques du Liban, la société pétrolière saoudienne Aramco…. Le cyber permet un mélange des genres incroyable, virulent et discret. Il est l'espace d'un néo-hobbésisme, celui de la lutte de tous contre tous.

Car voici en conclusion la grande interrogation stratégique du moment : celle de l'intensification de cette cyberconflictualité, remarquée par tous les observateurs : aussi bien en volume qu'en difficulté technologique, la cyberconflictualité se développe. Au point de poser

la question de l'escalade de la violence. Et si chacun admet qu'une guerre classique ait des aspects cyber, la question qui se pose désormais est la suivante : **une guerre cyber peut-elle déborder en guerre classique ?**

Le lecteur l'aura compris : le cyberespace introduit de nouvelles questions stratégiques et **tout comme il avait fallu du temps pour digérer la révolution stratégique nucléaire, il faudra du temps pour bien appréhender la révolution cyberstratégique**. Nous n'en sommes qu'aux prémices.

Plus

Olivier Kempf, *Introduction à la Cyberstratégie*, Paris, Economica, 2012.

4e de couverture

Le cyberespace nous environne et régit nos vies, au moyen bien sûr de l'Internet, mais aussi de tous les systèmes de télécommunication ou des réseaux (bancaires, médicaux, énergétiques, ...). Il nécessite une stratégie propre, la cyberstratégie.

La cyberstratégie est la partie de la stratégie propre au cyberespace, considéré comme un espace conflictuel où s'opposent, avec des techniques et des intentions variables, des acteurs différents (états, groupes, individus).

Ce livre expose les grands fondements de cette cyberstratégie : à partir des caractéristiques du cyberespace, il analyse les facteurs stratégiques (lieu, temps et acteurs) et leurs conséquences, avant de s'interroger sur les dispositifs stratégiques (le couple offensive/défensive, la cyberdissuasion, la géopolitique du cyberespace).

Premier ouvrage analysant en profondeur cette nouvelle discipline, il permet d'appréhender clairement ce nouvel espace stratégique.

. Se procurer l'ouvrage d'Olivier Kempf sur le site des éditions Economica

---

P.-S.

Maître de conférences à Sciences Po, conseiller éditorial de la *Revue Défense Nationale*, dirige la collection "Cyberstratégie" chez Economica. Il a publié *Introduction à la cyberstratégie* (Paris, Economica, 2012)

Notes

[1] L'usage admet d'utiliser l'apocope « cyber » pour désigner le cyberespace.