diploweb.com La revue géopolitique
ISSN : 2111-4307

Cyberespace : les trois âges

dimanche 8 janvier 2012,par François GERE

Citer cet article / To cite this version :
François GERE, **Cyberespace : les trois âges** , *Diploweb.com : la revue géopolitique, 8 janvier 2012.*

François Géré appelle de ses voeux une Cyberstratégie. Il la définit, à ce jour, comme « *l'ensemble des pratiques civiles et militaires, publiques et privées, intérieures et extérieures visant à aménager le cyberespace afin de répondre aux objectifs fixés par l'autorité politique pour assurer la prospérité et la sécurité de la communauté des citoyens, en conformité avec les impératifs de souveraineté et d'autonomie de décision nationales, dans le respect des libertés matérielles (économie) et spirituelles (idéologie)*.

A LA VEILLE de la Révolution française, l'abbé Siéyès publia un pamphlet fameux pour son commencement : « Qu'est-ce que le Tiers-Etat ? Rien. Que devrait-il être ? Tout ! » Ainsi en va-t-il aujourd'hui du Cyberespace dans lequel nous vivons, travaillons, pensons et communiquons de manière désormais si naturelle, si étourdie que nous ne prenons pas garde aux considérables implications de l'utilisation de ce domaine sans équivalent dans l'histoire de l'humanité. Rien de plus emblématique que les grands forums de relations internationales et de sécurité globale. D'entrée de jeu, on mentionne le Cybererspace, on salue son importance, on s'inquiète de sa protection. Mais une fois cet hommage rendu on en revient aux sujets traditionnels, abordés d'immuable manière selon des approches ronronnantes depuis deux siècles. Bien sûr, on aura pris soin, au détour du programme, d'organiser une table-ronde où les experts de la cyberdéfense se retrouvent entre eux comme à l'ordinaire. On doit à l'objectivité de relever que lesdits experts ont formé depuis deux petites générations une communauté volontiers repliée sur elle-même, soudée par l'usage d'un redoutable jargon fait de néologismes, d'acronymes, d'abréviations, pour la plupart américaines (pour ne pas dire californiennes). Elle a, cette communauté, ses rituels, ses modes, ses grand' messes, ses controverses et naturellement ses hérétiques. En somme, tout irait pour le mieux si depuis une demi-douzaine d'années l'action de perturbateurs majeurs ne venait non seulement causer des dégâts de toute nature mais, plus encore, troubler l'ordre des catégories traditionnelles de la stratégie.

1. L'âge de la Création

Le Cyberespace constitue un espace artificiel et universel, accessible à tous, en mutation technologique permanente couvrant tous les domaines de l'activité humaine.

Ceci pose un problème majeur de nature philosophique. Jusqu'à présent l'action de l'homme visait à maîtriser des milieux physiques (Terre, Mer, Air, Espace). Il lui fallait en comprendre les lois afin de d'inventer les instruments techniques permettant, en surmontant autant que possible les obstacles identifiés, de tirer le meilleur parti des ressources offertes par cette Nature pour les transformer en Culture ou, plus largement, en civilisation. Dans le Cyberespace l'homme-créature se retrouve soudainement face à lui-même, le créateur. Il n'est de difficultés que celles qu'il s'impose dans une recherche prométhéenne du toujours plus et mieux dont on se demande quelle est la finalité ultime : la prospérité, la domination ? Faute d'une réponse claire à cette question constatons que cet événement renforce, au moins dans un premier temps, la concurrence, la compétition, le jeu et l'agressivité. C'est bien pourquoi il importe que cet homme « dénaturé » du Cyberespace accepte de s'imposer des règles de comportement, des codes de conduite semblables à ceux qui ont inspiré les réglementations touchant au territoire, et aux espaces inhabités, sorte de patrimoine commun à l'ensemble de l'humanité. L'entreprise est compliquée par l'absence d'un socle commun extérieur à l'homme,

préalable à son action. Traditionnellement la physique naturelle des différents milieux procurait ce fondement. Dans le cyberespace il n'existe plus, sauf à se mettre d'accord sur une sorte de simulacre de matérialité du « territoire » du Cyberespace. Or ceci n'est plus une hypothèse d'école car à l'âge de la Création succède celui de l'action conflictuelle.

> Pour votre formation, bénéficiez de la playlist vidéo Diploweb.com des Stratèges français du XXe siècle présentés par François Géré : Jean de Lattre de Tassigny, André Beaufre, Charles Ailleret, Lucien Poirier et Pierre-Marie Gallois.

2. L'âge des affrontements

Les attaques se multiplient en quantité comme en qualité. Les mesures de protection ordinaires n'y suffisent plus, la répression ne dissuade guère. La prospérité économique, le fonctionnement des Etats, la paix et la guerre sont devenus les enjeux. A la criminalité ordinaire (plus ou moins organisée) s'ajoute désormais l'action d'acteurs de niveau étatique disposant de moyens et de compétences très élevées. L'espionnage prend une dimension nouvelle qui rompt avec les comportements classiques. La recherche du renseignement n'est pas seulement militaire, elle est aussi le fait des entreprises qui s'efforcent d'accéder aux secrets industriels des concurrents.

Rappelons quelques cas, désormais célèbres qui n'ont jamais été pleinement et ouvertement élucidés : Estonie, (crise diplomatique avec la Russie, 2007), Géorgie, (guerre avec la Russie,2008), Iran (attaque de la centrale nucléaire de Natanz par le virus STUXNET, 2010), France (espionnage du ministère français des finances, 2010), pour ne rien dire des attaques contre le Pentagone et ses contractants industriels comme Lockheed-Martin.

Les procédés sont souvent semblables et bien identifiés : déni d'accès par saturation (*botnets*) en recourant à des ordinateurs zombies, vers, virus, implantation clandestine de bombes logiques parfois introduites en amont dans les logiciels vendus à l'utilisateur. Les vecteurs sont « innocents » : soit l'Internet, soit de simples clés USB, soit encore les téléphones portables dotés de nouvelles applications comportant des failles béantes. Les réseaux sociaux ne sont que des outils de transmission qui servent à la diffusion des idées, de l'information, de la propagande et…. de la désinformation.

A ce stade, apparaissent plusieurs défis majeurs qu'il va falloir relever en jouant sur différents registres. D'une part la création d'un continuum associant protection-agression-dissuasion afin d'inverser la relation entre l'agression et la sécurité, d'autre part le développement de dialogues entre les Etats soit en bilatéral soit en multilatéral. Enfin se pose le problème particulièrement difficile de l'attribution dans un espace sans frontières où la localisation n'a pas valeur d'identification. Pour faire face s'élaborent ici et là des stratégies et des doctrines encore incomplètes et peu coordonnées tant au plan intérieur qu'international. Nombreux sont encore les Etats réticents à toute discussion de fond tandis que d'autres pratiquent le dialogue de sourds en se gardant de signer les conventions internationales (Convention de Budapest adoptée par le Conseil de l'Europe en novembre 2001). Il y a tout lieu de penser que cette période durera et que, de ses débordements, de ses excès mêmes, surgiront le besoin et la

volonté du Code. En établissant les fondements de la doctrine militaire, de la diplomatie coopérative, de l'éthique et du droit international nous pouvons nous diriger vers l'âge du Code.

> Voir aussi : Pascal Martin, L'action cyberoffensive comme nouvelle capacité au profit d'une diplomatie coercitive

3. L'âge du Code

A l'âge de l'affrontement doit succéder celui du Code. Entreprise complexe qui n'a rien de désespéré dès lors, c'est là tout l'enjeu, que le besoin s'en fait sentir.

Code civil, code pénal, code de la route, autant d'exemples de règles admises par les sociétés pour assurer leur bon fonctionnement. Les gouvernements s'y rangent dès lors qu'ils intègrent l'idée d'un intérêt commun. Au niveau individuel, les usagers font de même, par libre consentement, une fois convaincus qu'il y va de leur propre sécurité. Le code permettra de réduire la piraterie informatique en la marginalisant. Les Etats auront à s'engager à ne pas recourir à des sous-traitants, à des mercenaires de tous poils ou à de soi-disant nationalistes. Il faudra assumer des responsabilités d'Etat pour brider et punir les contrevenants selon les lois nationales. Mais au delà se pose la question du droit international. La diplomatie aura à se poser la question de la légitime défense au niveau des Nations-Unies de manière à définir l'agression provenant d'un domaine déterritorialisé. Une sorte de Convention de Genève du Cyberespace doit constituer, à terme un objectif majeur. Ces codes auront aussi à respecter les libertés fondamentales, notamment celle des opinions, la vie privée et, bien sûr, le libre jeu de l'activité économique, ce qui suppose l'utilisation légitime du cryptage des données.

Afin de satisfaire à ces multiples tâches la sécurité, à elle seule, ne suffit pas. Elle doit s'inscrire dans un cadre plus général contribuant à son renforcement. C'est pourquoi il est indispensable de mettre en place une Cyberstratégie outil indispensable afin de penser, de prendre en compte et de donner réalité à l'ensemble des enjeux qui occuperont les décennies à venir. Cette Cyberstratégie peut, provisoirement, se définir comme « *l'ensemble des pratiques civiles et militaires, publiques et privées, intérieures et extérieures visant à aménager le cyberespace afin de répondre aux objectifs fixés par l'autorité politique pour assurer la prospérité et la sécurité de la communauté des citoyens, en conformité avec les impératifs de souveraineté et d'autonomie de décision nationales, dans le respect des libertés matérielles (économie) et spirituelles (idéologie)* ».

Plus

. Voir l’article de Ludovic Aubut-Lussier, "La démocratie virtuelle ? Expériences, défis et enjeux"

. Voir l’article de Laurent Bloch et Christophe Wolfhugel "Géostratégie de l’Internet"

P.-S.

Agrégé et docteur habilité en histoire. Fondateur de l’Institut français d’analyse stratégique (IFAS). Chargé de mission auprès du directeur de l’IHEDN et de l’Enseignement militaire supérieur. Titulaire de la chaire CASTEX de Cyberstratégie