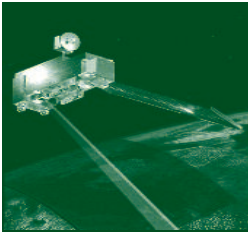




Stratégie dans le cyberspace

SOUS LA DIRECTION
DE FRANCOIS-BERNARD HUYGHE

DIRECTEUR DE RECHERCHE A L'IRIS



Quelle stratégie pour quel espace ?

Au moment où nous écrivons ces lignes, les médias font grand bruit de l'affrontement entre une hyperpuissance (les USA), une société commerciale (MegaUpload, un des 100 sites les plus fréquentés du monde, qui fournit du téléchargement gratuit) et Anonymous, un groupe militant international.

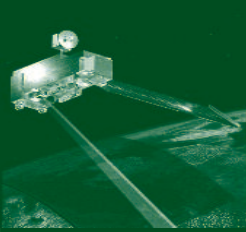
L'administration américaine a fait fermer le site (à Hong Kong) pour violation du droit de propriété intellectuelle et fait arrêter ses dirigeants (en Nouvelle Zélande). Conséquence immédiate : des militants ont bloqué plusieurs sites officiels par des « attaques distribuées de déni de service » (DDOS). Comment un État doit-il, et peut-il, répliquer ? Quelques jours auparavant, nous apprenions que des hackers anti-israéliens s'en étaient pris à des sites bancaires et des compagnies aériennes de l'État hébreu. En riposte, des cybermilitants sionistes du nom d'« Équipe des Forces de Défense Israéliennes » avaient frappé des sites saoudiens. Une fois de plus, étaient parus des articles expliquant que cette fois-ci enfin, ça y était ! La vraie cyber-guerre avait commencé ! Mais ces annonces ont lieu en réalité trois fois par an.

Bizarres conflits qui ne font pas de morts, qui bousculent les notions de frontière, qui mettent face à face des acteurs étatiques, des entreprises et des groupes militants, qui n'utilisent pas d'armes, mais des moyens de communication et dont on mesure mal la nocivité ni ne connaît bien les réels responsables. Les États-Unis ou Israël (qui parle ici de terrorisme) ou même le Japon (qui se dote d'armes pour y répondre) semblent bien décidés à les classer parmi les actes de guerre.

Qui dit conflit, dit stratégie ! Nous venons d'inaugurer en France une chaire dédiée à cette nouvelle discipline : la cyberstratégie. Plusieurs des auteurs de ce numéro ont par ailleurs participé à un colloque qui voulait poser les premiers jalons dans ce domaine. Mais comment raisonner dans le cyberspace ? Nous ouvrons le débat en présentant quatre points de vue.

Olivier Kempf se demande comment, ou s'il faut, transposer des concepts liés à la stratégie nucléaire comme celui de dissuasion. Eric Hazane nous rappelle ensuite que le cyberspace repose sur le monde réel et qu'il est régi par des codes comme la « grammaire » des protocoles. Barbara Louis-Sidney offre, de son côté, une vision juridique : comment une cyberattaque pourrait-elle être un acte de guerre ? Adrien Gévaudan s'insurge enfin contre l'idée de transposer dans le cyberspace des notions nées pour penser des milieux plus familiers introduisant la lutte des générations dans la cyberstratégie. ■

François-Bernard Huyghe



Cyberespace et espace nucléaire : ressemblances et dissemblances

*par Olivier Kempf,
Maître de conférence à l'Institut d'Etudes Politiques de Paris
Animateur du blog egeablog.net*

Depuis l'apparition du cyberespace et la notion conjointe de « cyberdéfense », les observateurs assimilent fréquemment le cyberespace et l'espace nucléaire. Ces quelques lignes veulent contribuer au débat, en comparant effectivement ces deux milieux, en interrogeant la notion de lutte technologique, enfin en apportant quelques remarques sur la notion de cyberdissuasion.

Cyber et nucléaire, même combat ?

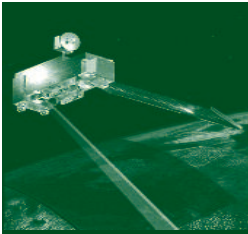
Le « nucléaire » est-il un milieu stratégique ou n'est-ce qu'un « domaine » ? Etant donné la prégnance qu'il a eue sur la stratégie depuis son apparition historique, nous admettrons qu'il s'agit d'un milieu, même si sa description topologique ou géographique est malaisée. Il est plus observé au travers de ses effets que de sa description directe. Mais on peut faire la même remarque pour le cyber : il s'agit là aussi d'un milieu anthropogène, construit par l'homme, même s'il repose sur des moyens techniques qui peuvent être géographiquement désignés.

Nombreux sont ceux qui voient alors des ressemblances entre le milieu nucléaire et le milieu cyber : ils partagent surtout l'illusion que ce nouveau milieu, comme tous les nouveaux milieux lors de leur apparition, engloberait tous les précédents : cela entraînerait, dès lors, par une sorte de nécessité, la règle selon laquelle celui qui domine le nouveau milieu domine l'ensemble du spectre stratégique et va donc gagner la guerre. C'est une illusion, dénoncée depuis longtemps par Colin Gray . Un nouveau milieu accroît la complexité de la stratégie générale, il rétroagit sur les autres milieux, mais il ne suffit pas

par lui-même à assurer la domination totale. Cela ne signifie pas cependant qu'il faut le minorer : la complexité accrue nécessite un effort de réflexion stratégique, comme le nucléaire l'exigea en son temps. Constatons d'abord que malgré la même couche technologique qui les fait se ressembler beaucoup (ce sont tous les deux des milieux artificiels), le nucléaire et le cyber présentent des différences qui tiennent justement à leur nature technique et scientifique.

Je crois en effet qu'il y a une dissemblance de taille : celle de l'incessante mutation technologique du cyber par rapport à la relative fixité du nucléaire. Certes, nous ne méconnaissons pas l'importance du passage de la bombe A à la bombe H, la présence de sous-marins nucléaires sous la calotte glaciaire, la miniaturisation qui a permis le missile ou l'invention du mirage : les innovations des quinze premières années du nucléaire ont forcé l'adaptation des concepts stratégiques. Pourtant la notion de dissuasion arrive très vite avec le nucléaire, même si elle subit des ajustements conceptuels réguliers (passage du primat nucléaire au conflit limité puis des représailles massives à la riposte graduée). Après, les concepts ont connu une relative fixité, probablement due à la fixité technologique.

Le cyber donne au contraire l'impression d'une constante lutte technologique où la course aux armements, à la différence de l'époque nucléaire, ne se fait pas seulement à la quantité (la loi de Moore) mais aussi à la qualité (qui est d'ailleurs, pour une part, la conséquence de la première). Il y aurait sans cesse croissance technologique dans le cyber, là où elle était finalement plus lente dans le nucléaire. ■■■



■■■ Cette idée peut bien sûr être critiquée, de deux façons, que j'aborde avec prudence car je n'ai pas les compétences techniques : mais un article ne sert-il pas à soumettre des hypothèses à débat ? J'accepte tout à fait la critique et la sollicite même, car elle permet de construire à plusieurs notre compréhension des choses.

Lutte technologique ?

La première objection serait que les architectures basiques usitées dans tous les systèmes informatiques seraient partout similaires et donc communes, ce qui rendrait factice la course technologique. J'ai toutefois le sentiment que si l'infrastructure semble commune (et facilement attaquable car nativement mal conçue pour la sécurité), les superstructures ont tendance à se différencier. Alors, l'évolution qualitative porterait sur les superstructures. La difficulté porterait donc sur la possibilité de percer ces superstructures, pour atteindre un noyau qui serait plus facile à détruire. Je laisse cette question aux spécialistes, mais la réponse emportera des conséquences stratégiques différentes.

La deuxième objection expliquerait que l'augmentation croissante de complexité accompagnerait, à peu près au même rythme, les progrès de la technologie : au fond, les deux se développeraient simultanément, selon une logique homothétique. Dès lors, la complexité croissante irait de pair avec les outils à même de la contrôler. Autrement dit encore, si cette hypothèse est vraie, elle relativise l'impression de course technologique aux armements cyber : mais elle ne l'invalide pas. En effet, si les moyens techniques accompagnent le développement de l'informatique, la présence croissante de ceux-ci est une réalité acceptée par tous : celle d'une complexité croissante (au sens propre, cyber) même si elle dispose pour cela des outils nécessaires (au sens propre, l'informatique).

Cyber-dissuasion ?

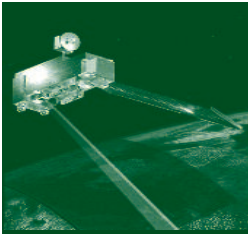
On peut donc dénoncer l'assimilation fréquente au fait nucléaire, qui se traduit le plus souvent

par la notion de cyber dissuasion. Je ne crois pas que la dissuasion soit un modèle pertinent pour le milieu cyber. Il faut tout d'abord revenir aux définitions. Selon le glossaire interarmées de terminologie opérationnelle, la dissuasion est le « fait de persuader un agresseur potentiel que les conséquences d'une action coercitive ou d'un conflit armé l'emporteraient sur les gains escomptés. Cela nécessite le maintien d'une puissance militaire et d'une stratégie crédible reposant sur une volonté politique nette d'agir ». Juste après, une définition de la dissuasion nucléaire précise l'application particulière au milieu nucléaire. On le voit donc, la notion de dissuasion recouvre deux choses :

D'une part la notion de riposte à une attaque. Elle entraîne que l'on ne défend pas seulement, mais que l'on passe à l'offensive. La chose mérite d'être précisée, tant la question de l'offensive paraît aujourd'hui plus ou moins tue dans la pensée stratégique francophone. Cela ne signifie pas qu'elle n'est pas possible, juste qu'elle doit être pensée.

D'autre part, la dissuasion a pour corollaire la notion de dissymétrie, puisque la riposte que l'on se propose d'asséner à l'adversaire occasionnerait des dégâts plus élevés que l'attaque que l'on nous porterait. Or, cette dissymétrie paraît aujourd'hui pour le moins difficile à prouver. Cette preuve est pourtant à la base de la crédibilité (même si la dissuasion nucléaire emporte une part d'ambiguïté rhétorique, qui lui est inhérente).

Crédibilité, voilà le dernier mot ! La crédibilité doit être technique, mais aussi stratégique. En effet, le dernier élément de la définition est le couple unissant une stratégie crédible et une volonté politique. Or, le politique n'a pas eu encore à se pencher sur ces choses là. Cela ne veut pas dire qu'il n'y a pas réfléchi : simplement qu'en France, il ne s'est pas exprimé publiquement dessus. Aussi me semble-t-il opportun de regarder encore cette notion de cyber-dissuasion, d'y réfléchir avec attention et circonspection, même si elle est beaucoup employée outre-Atlantique et que beaucoup la reproduisent, peut-être trop rapidement. ■



Cyberespace : définition et limite

par *Eric Hazane,*
Spécialiste Sécurité de l'Information et Cybersécurité

Si la géographie, l'histoire et le droit (international, de la mer, aérien, etc.) nous permettent d'appréhender facilement les Etats dans leurs frontières, le cyberespace, lui, ne se laisse pas facilement apprivoiser ! Hybride de par ses caractéristiques physiques et virtuelles, hétérogène par la diversité des équipements permettant d'y accéder, mutable de par ses constantes évolutions et sa croissance folle, l'application de modèles et d'outils d'analyse classiques est au mieux partielle quand elle n'est tout simplement pas inadaptée donc inapplicable.

Dans ce cadre, le cyberespace doit être envisagé en renouvelant la pensée avec de nouveaux outils. En prenant comme point de départ les travaux de Jean-Lou Samaan, qui propose un modèle sur trois niveaux (lexical, syntaxique, sémantique), on trouve la notion d'encapsulation et d'isolation des couches que l'on retrouve également dans le modèle OSI (pour l'interconnexion en réseaux des ordinateurs). Les deux modèles en ont commun la prégnance de caractéristiques essentiellement physiques avec une notion de « syntaxe » (protocoles, techno-

logies). Intéressant, ce modèle en couches n'apporte cependant pas la profondeur nécessaire pour aborder le cyberespace.

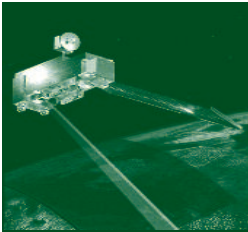
Maitriser un territoire ambigu

En utilisant des notions de géographie et de géopolitique, il est possible d'identifier des domaines qui, sans être forcément exhaustifs, vont nous aider à mieux cerner le cyberespace. A travers les zones physiques formées par les infrastructures des réseaux et les milliers de Systèmes d'Information isolés derrière leurs bastions sécurisés (filtrage des flux, détection d'intrusions, anti-virus, etc.), se découvrent des territoires isolés donc des frontières. Mais aussi les acteurs, internautes, criminels et surtout Etats. Enfin des ressources et des intérêts, très souvent divergents, générant de la malveillance, de l'appropriation illégitime voire des conflits.

Si la géographie et la géopolitique fournissent des outils relativement efficaces, n'oublions pas la dimension juridictionnelle sans qui les règles du jeu ne peuvent exister, même dans le cyberespace. En-

visagées à l'orée des années 2000 dans le cadre d'une autorité supranationale (ONU), les intérêts politiques voire stratégiques de certaines nations n'ont logiquement mené qu'à une impasse. Une certaine dose de régulation semble cependant nécessaire, ne serait-ce que pour éviter la militarisation, possiblement en cours, du cyberespace (Stuxnet, Duqu...). Le fait que l'OTAN se soit emparée du sujet à travers les Global Commons n'est peut-être pas un si mauvais signal en soi : si tout ou partie du cyberespace vient à considérée comme un « bien commun de l'Humanité », peut-être que l'usage d'armes non-cinétiques restera l'exception. Sinon, issues d'un domaine aux frontières pas si virtuelles que cela, leurs effets pourraient avoir un impact plus ou moins dévastateur... dans le monde réel. ■

N.B.: l'auteur tient à remercier Arnaud Garrigues, auteur de « Géo-Analyser le cyberespace »



Quelles perspectives d'évolution pour le droit encadrant les conflits informatiques ?

*par Barbara Louis-Sidney,
Chargée de Veille stratégique et d'analyses juridiques à la CEIS*

Lorsque certains Etats, comme les Etats-Unis, affirment qu'ils riposteront systématiquement à toute attaque informatique contre leurs infrastructures critiques, la question du fondement juridique de cette affirmation se pose naturellement.

Le raisonnement tenu par les Etats-Unis consiste, en effet, à considérer que toute riposte à une attaque informatique touchant leurs infrastructures critiques sera encadrée par la légitime défense internationale, envisagée notamment dans le cadre du droit des conflits armés. Mais si, en théorie, rien ne s'oppose à l'application du droit des conflits armés en matière d'attaques informatiques, en pratique, l'exercice se révèle relativement complexe. Celui qui voudra recourir à la légitime défense pour riposter face à une cyberattaque devra prouver qu'il est en présence d'une agression armée. Entendons par là, sans rentrer dans les détails, que l'attaque devra être « armée », revêtir une certaine intensité et être attribuée à un Etat ou à un agent travaillant pour son compte ou sous son contrôle effectif.

Trois idées pour adapter le droit

Le décor est ainsi clairement posé : le raisonnement par analogie semble difficilement applicable à une cyberattaque pure et simple. En effet, si le caractère armé d'une cyberattaque peut être supposé en cas d'emploi d'un code malveillant, le critère de l'intensité reste complexe à apprécier et l'attribution de l'attaque relativement hasardeuse. Face à ces freins, le droit des conflits armés, certes pleinement applicable en théorie, risque de rester inappliqué en pratique. Sauf à en-

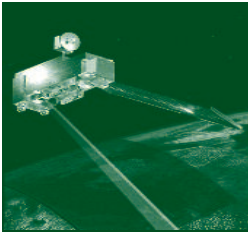
visager une évolution du droit. Cette évolution, loin de tout révolutionner en la matière, consisterait à simplifier l'application du droit déjà existant aux conflits informatiques. A cet égard, trois idées peuvent être développées.

Idee n°1 : Faire évoluer la notion d'agression.

Disposant d'un large pouvoir d'appréciation, le Conseil de sécurité de l'ONU a la possibilité d'inclure dans l'actuelle notion d'agression des formes d'emploi de la force non encore envisagées. Cela permettrait d'ajuster la notion d'agression aux spécificités de l'attaque informatique ; de développer des critères propres à ce que l'on appellerait une « agression informatique ». Ces critères, tenant compte de la nature de basse intensité de la cyberattaque pure et simple, utiliseraient une échelle d'intensité plus adaptée. Baisser de quelques crans le niveau d'intensité exigé pour qualifier une attaque informatique pure et simple d'agression armée permettrait, dans l'absolu, l'exercice d'actes de légitime défense.

Idee n°2 : Passer outre la problématique de l'attribution de l'attaque informatique.

La question de l'attribution de l'attaque est une préoccupation majeure en matière de conflits informatiques. En effet, sans attribution, pas de qualification de la nature de l'attaque informatique (cyberguerre, cyber-terrorisme, hacktivisme, etc.), ni d'engagement de la responsabilité d'un auteur (étatique ou non-étatique), ou de riposte efficace. Aujourd'hui, aucune solution technique d'identification de l'auteur d'une attaque n'est infaillible ■■■



■■■ (falsification d'adresses IP, techniques d'anonymisation diverses...). Le réseau Internet, maillé par nature, implique que certaines cyberattaques transitent par des infrastructures situées sur des territoires distincts. Plusieurs pays peuvent ainsi être identifiés comme étant la source d'une cyberattaque. Remonter jusqu'à l'auteur de l'attaque peut donc s'avérer difficile, voire impossible. Dans ce cas précis, à défaut de moyen technique, il est possible de recourir à un montage juridique. Ce montage ferait appel à des notions existant déjà.

L'article 3, f) de la résolution 3314 de l'ONU définissant l'acte d'agression dispose en effet que « le fait pour un Etat d'admettre que son territoire, qu'il a mis à disposition d'un autre Etat, soit utilisé par ce dernier pour perpétrer un acte d'agression contre un Etat tiers [...] réunit les conditions d'un acte d'agression ». Cette solution, également proposée par le Centre d'excellence de Tallin, permet de considérer comme responsable un Etat ayant toléré une action illicite sur son territoire. Elle a le mérite de passer outre l'impérieuse exigence de l'identification de l'auteur de l'attaque. Elle a également le mérite de mettre au cœur des préoccupations la lutte contre la cybercriminalité à l'échelle nationale. En présence d'une telle disposition, les Etats seraient en effet contraints de veiller à lutter efficacement contre tout acte de criminalité informatique, puisque, au-delà de leurs finalités divergentes, les cyberattaques ont en commun leurs outils (vers, virus, etc.). La lutte contre la cybercriminalité apparaît ainsi complémentaire à toute stratégie de cyberdéfense nationale.

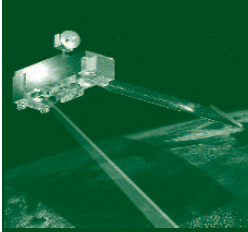
Idee n°3 : « Codifier » les dispositions existantes et applicables au cyberspace.

Il n'y a pas de vide juridique dans le cyberspace. Les attaques informatiques peuvent faire l'objet de l'application de nombreux textes internationaux. Internet n'est pas une abstraction. Et bien que les informations qu'il transporte soient par définition immatérielles, ce gigantesque réseau de réseaux s'appuie sur des infrastructures physiques,

soumises à des accords internationaux. Les attaques informatiques, en fonction de leur intensité ou encore de leur auteur, sont susceptibles de déclencher l'application de différents types de corpus juridiques. S'appliquent le droit international humanitaire en cas de conflit armé et d'autres textes internationaux en cas de conflit non armé. Une attaque qui n'est pas qualifiée par le Conseil de sécurité d'« agression armée » reste susceptible d'engager la responsabilité d'un Etat sur le fondement d'un fait internationalement illicite, pour non-respect de textes internationaux actuellement en vigueur (voir : projet d'articles sur la responsabilité de l'Etat pour « fait internationalement illicite » adopté en 2001). Citons : la Déclaration universelle des droits de l'homme ; le Pacte international relatif aux droits civils et politiques ; la Convention Européenne des droits de l'Homme ; la Convention de l'UIT de 1992 ; la Constitution de l'UIT de 1992 ; les Règlements des radiocommunications de 2007 ; la Convention sur l'emploi de la radiodiffusion dans l'intérêt de la paix de 1936 ; la Convention de Montego Bay de 1982 ; la Convention internationale relative à la protection des câbles sous-marins de 1884 ou encore le Traité de l'espace de 1967.

Contre toute attente, cette liste, non-exhaustive, de textes disposant chacun de quelques articles applicables au cyberspace ne facilite pas la tâche des acteurs d'Internet. Il est en effet difficile de s'y retrouver. Le cyberspace nécessite une clarification de son régime juridique. Clarification qui pourrait être apportée par la réalisation d'un traité dédié.

Ce traité rassemblerait, à la manière d'une codification, les dispositions applicables au cyberspace et disséminées dans cette myriade de textes internationaux. Ce traité présenterait aussi, pourquoi pas, une vision plus claire de l'agression informatique, si tant est qu'elle existe (ou qu'elle soit reconnue un jour par le Conseil de sécurité de l'ONU). On peut citer comme précédent l'article 1^{er} du protocole du 26 juillet 1975 qui, amendement le Traité de Rio, définissait un type d'agression ■■■

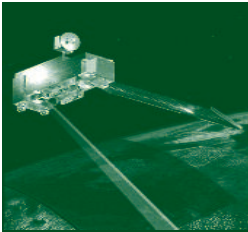


■■■ en se fondant sur la résolution 3314 de l'ONU. Le document pourrait reprendre le principe du droit de l'espace exigeant son utilisation à des fins pacifiques, tout en y assortissant des exceptions telles que la légitime défense informatique, évitant ainsi le raisonnement par analogie décrit ci-dessus.

De telles évolutions ne peuvent se faire sans l'assentiment des Etats. Mais ces derniers sont-ils réellement susceptibles de s'engager dans de telles réformes ? La faiblesse de la notion d'agression n'est peut-être pas un défaut majeur du droit. La conserver en l'état limite le champ d'application de la légitime défense informatique et, de

fait, exclut l'éventuelle justification légale d'actes de riposte entre Etats. D'un autre côté, conserver le droit tel quel leur permet surtout d'agir en toute impunité dans le cyberspace. Deux raisons pouvant expliquer l'inertie des Etats. En l'absence d'évolution du droit écrit, il est probable que se développent sur le long terme des usages qui constitueront peut-être les fondements d'une coutume internationale. Il est donc de l'intérêt des Etats d'affirmer dès aujourd'hui sur la scène internationale leurs stratégies de gestion des cyber-conflits. ■

*
* * *
*



Relations internationales et cyberstratégie : la tentation moutonnaire

par **Adrien Gévaudan**,
Fondateur du site intelligence-strategique.eu

L'histoire des relations internationales montre que l'influence d'un pays dépend en grande partie de sa capacité à assimiler les innovations technologiques et à les intégrer dans une perspective global(isant)e. Il y a des pays qui ont compris ce principe, et d'autres qui loupent le coche. Les premiers se dotent d'un avantage stratégique décisif, quand les seconds passent leur temps à combler leur retard ; quand ils ne nient pas, purement et simplement, l'importance du tournant qu'ils ont pourtant manqué.

Stratégie, influence et innovation

La puissance forte cherchera à conserver l'avantage qu'elle possède en investissant massivement dans l'innovation qu'elle a perçue comme décisive. La moyenne, inquiète de voir le rapport de force se creuser avec la première, tentera de l'imiter, au risque de s'inscrire dans la réaction plus que dans l'action, et donc de ne jamais faire preuve d'imagination. La faible, enfin, aura à cœur de saisir l'occasion de

comblent, au moins dans un domaine, l'écart de puissance qui la sépare des deux premières ; elle prendra pour cela des risques importants, dont certains se révéleront payants, et sera définitivement force de proposition et facteur d'innovation.

Ainsi, Superpuissance et Micropuissance sont les deux idéaux-types de pays les plus susceptibles de contribuer à des percées décisives, dans quelque domaine que ce soit ; la première de par la confiance et les moyens que lui confèrent les avantages de son statut, la seconde avec l'énergie du désespoir. Il ne fait jamais bon être une puissance moyenne. Adeptes des comportements moutonniers, elle se trompe souvent de débat, pérorer, et la tentation d'imiter le fort aura tendance à lui ôter toute imagination.

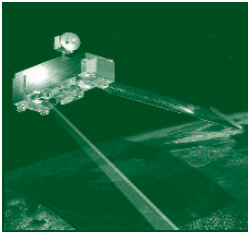
La France et le cyberspace

Le cyberspace, en tant que lieu virtuel, est le nouvel environnement à occuper. Sa maîtrise est un enjeu stratégique majeur pour chaque Etat

désirant maximiser son influence. Conformément à la tendance énoncée dans les précédents paragraphes, certains l'ont vite compris, quand d'autres tentent de suivre les locomotives technologiques.

Où est la France dans tout cela ? Puissance moyenne par excellence depuis un siècle (et souvent frustrée de cela), est-elle tombée dans le piège confortable de l'imitation des puissants, ou a-t-elle su avoir l'intelligence de saisir rapidement les opportunités que lui offrait l'irruption du cyberspace dans les relations internationales ?

S'il est évident que seule l'Histoire permet de lever le voile sur les stratégies étatiques, le secret ne doit pas nous empêcher de nous interroger sur la réalité d'une situation. Un pays ne dévoilera ses grandes orientations stratégiques que s'il y voit un intérêt : orchestration d'une propagande, afin de faire croire qu'il ne fait rien de plus que d'autres Etats ; désinformation classique, dans le but de tromper ses adversaires sur ses



■■■ priorités ; ou bien même, psychologie inversée oblige, transmission d'informations (relativement) véridiques mais sur lesquelles on fait planer un doute raisonnable, laissant supposer aux autres Etats que telle n'est pas la réalité.

Les seules informations en sources ouvertes concernant la stratégie française en matière de cyberdéfense ne nous permettent pas d'être optimistes quand à sa place dans ce nouveau concerto international. Les colloques, séminaires et autres conférences se caractérisent par une tendance absolument stupéfiante au verbiage et à l'aveuglement.

Verbiage, car les intervenants s'occupent bien trop souvent de sémantique, et jamais de technique. Aveuglement car le présumé dominant est que l'espace cyber se doit d'être appréhendé comme un nouvel espace classique (terre, mer, air, espace), susceptible d'être contrôlé par les mêmes méthodes ; alors même que la logique voudrait que, ne répondant à aucune des règles physiques et sociologiques traditionnelles, il soit l'objet d'un intense travail théorique.

Il faut dépasser le simple cadre de la réflexion. Il faut agir... et non, se contenter de définir ou redéfinir un sous-espace. Ce n'est pas en ergotant sur des termes qu'une stratégie

claire peut être définie ; ce n'est pas en inventant des concepts à chaque instant ni en recyclant des termes d'autres disciplines (« coalescence », « fractal » et autre « hologrammatique ») que l'horizon international d'une puissance moyenne comme la France s'éclaircira. Enfin, ce n'est pas en ajoutant « cyber » devant chaque notion traditionnelle, et/ou « stratégique » à la fin de chaque phrase que le fossé avec les grandes puissances se comblera.

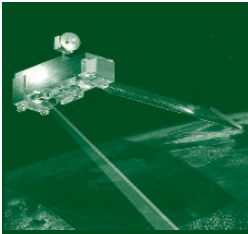
Décalage générationnel

Pourtant, force est de constater l'extrême compétence de nombreux experts francophones, le pays regorge de talents, de volontés d'innovation et de changement ; alors pourquoi cette lenteur bureaucratique ? La montée en puissance de l'Allemagne pré et post-bismarckienne a coïncidé avec l'arrivée au pouvoir de jeunes aux idées nouvelles, il s'agit de s'interroger sur le difficile renouvellement des générations qui caractérise la France actuelle.

De nouvelles idées supposent bien souvent de nouvelles personnes. Or, le microcosme de la cyberstratégie est (sur)occupé par des intervenants, certes très intelligents et passionnés, mais plus prompts à tenter de calquer leurs anciennes stratégies classiques sur le nouvel es-

pace cyber qu'à essayer de penser autrement.

Peut-être tout cela participe-t-il d'une stratégie extrêmement complexe de déception (au sens anglo-saxon du terme), et les programmes de cyberstratégie français sont-ils en réalité à la pointe ; peut-être font-ils jeu égal avec leurs équivalents américains, chinois et israéliens. Mais il est également possible, pour ne pas dire probable, que les informations disponibles en sources ouvertes sur la cyberstratégie française reflètent un tant soit peu la réalité, et que le pays soit tombé dans le piège classique et confortable de la puissance moyenne moutonnaire. Dans ce cas, seule l'union de talents aussi différents et complémentaires que des experts en sécurité informatique, en relations internationales, en stratégie et en géopolitique peut permettre à la France, non pas de rattraper un quelconque retard (car cela [pré]supposerait une vision linéaire), mais de créer sa propre voie/voix dans un monde où les conflits asymétriques viennent de trouver un nouvel espace d'expression. ■



Réinventer la guerre...

*par François-Bernard Huyghe,
Directeur de recherche à l'IRIS*

Pendant des siècles, la stratégie a consisté à disposer des forces dans l'espace. L'usage de la violence renvoyait à la question de la distance donc du temps : comment faire arriver ma charge de cavalerie au moment où son flanc droit sera dégarni ? Comment faire parvenir mes missiles sur leur cible sans qu'il les arrête en route ou qu'il me contre ?

Se posait comme corollaire la question du contrôle territorial : comment tenir le sommet de cette colline, position dominante ? Comment couper les routes maritimes adverses ? Comment, au final, occuper sa capitale ? Dois-je garantir le territoire de mes alliés européens contre une attaque classique en risquant l'Apocalypse nucléaire ? Comment sanctuariser ? Comment tenir l'orbite d'où mes satellites pourront sécuriser mon espace (guerre des étoiles) ?

C'est pourquoi l'idée que la guerre après s'être déroulée sur terre, sur mer, dans les airs et (potentiellement) dans la stratosphère, gagne maintenant le cyberspace, cette idée si logique en apparence nous embarrasse tant. Laissons de côté la question de savoir s'il existe vraiment une cyberguerre – elle ne fait pas de cybermorts, ne débouche pas sur des cyberpaix, n'est pas forcément menée par des cyberarmées, etc.

L'attaque dans le cyberspace présente la particularité de suivre un trajet instantané (ou d'agir à retardement comme certains virus). Mais aussi d'emprunter pour cela divers relais difficiles à retracer. Par exemple, une attaque par déni d'accès peut transformer en zombies des milliers d'ordinateurs de plusieurs pays. Quant au territoire, il n'est facile de savoir ni si celui qui est touché était vraiment (ou uniquement) celui qui était visé, ni de quel territoire et sous la responsabilité de quelle autorité sont parties les attaques.

Tracer, identifier, interpreter...

Du coup, la cyberattaque emprunte la logique de l'espionnage – acquérir une information en dépit des défenses de ceux qui la possèdent – ou du sabotage – empêcher les systèmes informationnels adverses de fonctionner –. Mais elle en emprunte aussi le principe du secret et de la clandestinité. Quand l'attaquant est anonyme ou multiplie leurres et relais pour tromper la riposte, la question plus policière que militaire du « qui l'a fait ? » devient cruciale. Tracer, identifier, interpreter... Autant de défis pour une réflexion stratégique encore naissante. ■

L'Observatoire Géostratégique de l'Information

Sous la direction de François-Bernard Huyghe, cet observatoire a pour but d'analyser l'impact de l'information mondialisée sur les relations internationales. Comprendre le développement des médias et de l'importance stratégique de la maîtrise de l'information. Il analyse, par exemple les rapports de force entre puissances politiques et économiques et les firmes qui contrôlent le flux des informations dans le Monde.

IRIS - Institut de Relations Internationales et Stratégiques

2 bis, rue Mercoeur
75011 Paris - France
iris@iris-france.org

www.iris-france.org
www.affaires-strategiques.info

Secrétariat de rédaction : Pierre-Yves Castagnac