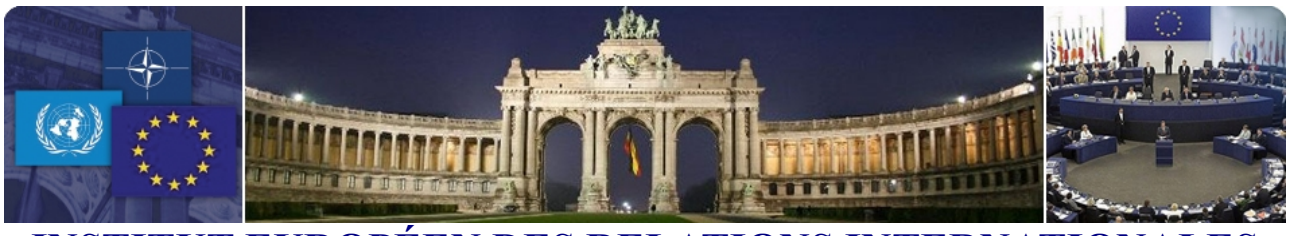

INSTITUT EUROPÉEN DES RELATIONS INTERNATIONALES

WORKING PAPER

5-2014

LA GÉOPOLITIQUE À L'ÂGE NUMÉRIQUE

DISCOURS D'INTRODUCTION

SIXIÈME CONFÉRENCE DE LA ONZIÈME ANNÉE DE L'ACADEMIA DIPLOMATICA EUROPAEA

13 FEVRIER 2014

Irnerio SEMINATORE

Président de l'Institut Européen des Relations Internationales (IERI)

Directeur de l'Academia Diplomatica Europaea (ADE)

Bruxelles

14-02-2014

Bruxelles, 14 Février 2014

Institut Européen des Relations Internationales

27/A, Boulevard Charlemagne

1000 – Bruxelles (Belgique) Tel. : +32.2.280.14.95 – Site Web : www.ieri.be

Citation : Irnerio SEMINATORE, La G*éopolitique à l'Âge numérique*, N° 5-2014, *IERI Working Papers*, Bruxelles, 2014

INSTITUT EUROPÉEN DES RELATIONS INTERNATIONALES

LA GÉOPOLITIQUE À L'ÂGE NUMÉRIQUE

Irnerio SEMINATORE

INTRODUCTION

La géopolitique des réseaux de l'âge numérique ne sera pas le reflet des alliances militaires du XXème siècle, car les figures des attaquants et des cibles ne seront plus seulement les États et l'Intelligence personnalisée des États au sens clausewitzien du terme. En effet, les figures classiques du conflit, les États porteurs de calculs rationnels et d'une espérance de gain politico-stratégique seront rejoint par des attaquants individuels, rendant opaque l'origine et « le signe politique » de la frappe. Ainsi, la logique du déséquilibre des forces sera renversée par le retour de la symétrie et par la « guerre Hobbesienne de tous contre tous ».L'asymétrie des forces était recherchée par les stratèges classiques. Et cependant elle représentait une contrainte, la concentration du tir sur les cibles.

La cyber-guerre se configure comme une rupture stratégique en raison de ses caractéristiques : universalité de son champ d'action et multiplicité des opportunités consenties à l'attaquant. Pour bon nombre d'analystes, le champ de bataille du futur sera le cyber-espace. On peut se demander si les virus informatiques remplaceront la balistique, l'atome et les armes à feu. Questions légitimes car la lutte informatique offensive sera conduite par des combats non lethales, non codifiés et opaques, obéissant à des signaux politiques à visées stratégiques.

Si le réseau global du Cyber-espace devient le lieu d'une confrontation majeure et donc le début d'une « guerre hors limites » imaginée par les Colonels chinois Quiao Liang et Wang Xianghui en 1999, une attaque, planifiée et massive sur le cyber espace peut-elle déborder en une guerre classique ? Or, il faut se rappeler que tous les réseaux interconnectés à internet (fibres optiques) participent du cyberespace qui est non seulement le champs dématérialisé d'une virtualité omniprésente dans l'organisation de la vie collective mais aussi un terrain d'hybridation avec toutes les structures informationnelles de la société.

En raison de l'irruption d'une myriade d'acteurs individuels dans les pulsations politiques de la mondialisation ces individus s'associent dans des occasions imprévisibles, en « coalitions de circonstance », provocant des basculements politiques mimétiques (les révoltes arabes). Plusieurs facteurs entrent en jeu pour définir ce nouveau champ stratégique :

- les flux des acteurs étatiques et individuels
- l'opacité dans l'attribution de l'action et de son origine
- la non léthalité de la frappe
- le ciblage infrastructurel et désorganisateur des actes
- la liberté de l'initiative

Ainsi, le retour de l'offensive, l'allongement du temps stratégique de préparation et d'anticipation et l'effet dévastateur qui n'est pas immédiat. Par sa virulence et par sa discrétion, cette intensification de la cyber-conflictualité peut-elle se détourner et se dévoyer par une action de préemption discrète ? Dans ce cas serait affermie la supériorité de la stratégie indirecte (Liddell-Hart et Beaufre) sur la stratégie clausewitzienne et directe.

La grande question sous-jacente peut se résumer en peu de mots. La révolution induite dans la stratégie par l'informatique, est-elle de même nature que la révolution induite dans la stratégie par l'atome ? Si l'atome a valorisé et porté à l'extrême la défensive et la dissuasion, bref le concept de non-guerre, et a fait naître une forme particulière de menace et de diplomatie (la diplomatie de la coercition – Shelling), la stratégie informatique, par son opacité et sa discrétion, laisse-t-elle un espace à la diplomatie, à la modération et à la politique étrangère ?

La particularité de l'intelligence du XXIe siècle est celle d'opérer, en support de la décision, comme couverture de surveillance stratégique à caractère permanent. Celle-ci est actée dans les deux fonctions de la « défensive » et de l'« attaque préemptive ». Ainsi, le contexte mondial dans lequel s'inscrira toute action offensive de grande ampleur conjuguera les antagonismes rationnels des États, les rivalités hégémoniques des acteurs majeurs de la globalisation, les actions de représailles et les stratégies géopolitiques mises en œuvre par les services électroniques et d'espionnage dans le cadre d'une compétition économique acharnée, et de formes renouvelées de mésententes

idéologiques, mêlées à des actes de piraterie patriotiques. Des « chocs », traditionnels ou extrémistes, doublés de nouveaux conflits urbains, intracommunautaires et ethniques, s'ajouteront à ces scénarios perturbateurs.

À la lumière de ces hypothèses, les menaces apparaîtront pour ce qu'elles sont : des conflits non déclarés et des dangers imminents à potentiel de létalité élevée. La « menace informatique » y jouera un rôle soft et impalpable, comme aveu implicite d'une paralysie des appareils économiques et sociétaux, lancés dans les dynamiques des interdépendances. L'usage offensif des réseaux informatiques mondiaux a été codifié par un rapport, « La guerre off-limits » des Colonels chinois Quao Liang et Wang Xiangsui en 1999. L'énoncé essentiel de ce rapport se résume au concept de « guerre sans restrictions » ou encore « sans normes ».

L'« INTELLIGENCE STRATEGIQUE »
VERS UN RENFORCEMENT DE LA SOUVERAINETE

Par ailleurs, puisque la gestion et la solution des conflits se décideront de plus en plus sur le terrain de l'information, et puisque la sécurité militaire et la sécurité économique passent nécessairement par un vecteur commun, celui de l'intelligence et de la connaissance globale (universités, écoles supérieures, services publics d'intelligence, bibliothèques, monde des affaires), l'autonomie de ce vecteur deviendra cruciale.

LA MENACE INFORMATIQUE ET LA CYBERGUERRE

La menace informatique revêt deux formes distinctes. La première est identifiée à la capacité de mener une attaque de masse aux infrastructures adverses par saturation des ordinateurs visés. La deuxième, ciblée, opère à la manière d'un cheval de Troie. Celle-ci est caractérisée par l'intrusion des flux d'informations sortants, plus ou moins discrets. Il s'agit d'attaques détectables qui permettent d'observer les méthodes et techniques de défense et de réaction à l'attaque[1].

1La guerre de l'information électronique exige une série élevée de capacités :

- l'identification préalable des secteurs-clés, civils et militaires de l'adversaire, à forte valeur incapacitante ;
- la maîtrise des techniques d'intrusion des infrastructures informatiques critiques ;
- un professionnalisme élevé ;
- une planification et coordination de l'attaque, massive et périodique ;
- le contournement des dispositifs de surveillance et de cryptage ;
- l'utilisation éventuelle de « réseaux dormants », au sein des « sites » d'industrie de technologies avancées et des secteurs de production d'ordinateurs.

Le principe capital de la menace, puis de l'attaque informatique repose sur sa forme résolument offensive, coordonnée et directe. La clé doctrinale de la « guerre off-limits » est l'absence de règles, le rejet des normes, la permissivité totale des formes d'intrusion, la convertibilité de tout outil à des fins de combat et de conflit, l'utilisation stratégique de l'« intelligence » et de l'espionnage, civil et militaire, l'orchestration et la mobilisation collectives de toutes les ressources humaines disponibles, le culte de l'héroïsme et des valeurs martiales à des buts individuels d'emploi offensif et à des fins collectifs de dominance cybernétique.

Du côté de l'Occident, penchent négativement l'absence de réflexes d'autodéfense et les faux calculs économiques et diplomatiques, la dégradation rapide des conditions de protection face à la sophistication des méthodes employées et à la création au sein de certaines armées (APL par exemple), des secteurs importants, ayant pour objectif la pénétration, l'espionnage, la destruction ou la mise hors d'usage de pans entiers d'activités privées ou publiques. Un constat patent face à une série d'actes offensifs, ayant touchés plusieurs pays occidentaux (Estonie, Allemagne, France, États-Unis, Japon, Nouvelle-Zélande, etc.) résulte de ces actions offensives.

Ces avertissements et formes d'attaques diverses ont testé les vulnérabilités des infrastructures et des réseaux informatiques occidentaux. En effet, une nouvelle forme de conflit vient de naître, depuis une vingtaine d'années, la guerre d'information électronique ou « cyberguerre ». Théorisée et codifiée, elle travaille à l'interruption et à la neutralisation de l'ensemble des transmissions, câblées ou satellites, basées sur la méthode « dianxe », selon laquelle l'atteinte d'un point vital de l'adversaire, pratiqué dans les arts martiaux, permet d'incapacité totalement l'adversaire. Au plan diplomatique, la méthode de gestion du monde comme espace de puissance et, en même temps, comme protection d'influence se fait valoir par le linkage horizontal ou vertical.

Au seuil d'un conflit majeur futur, trois types de menaces se transformeront en attaques immédiates, simultanées et préventives :

- les menaces cybernétiques ;
- balistico-satellitaires et terroristes ;
- les attaques sous-marines.

La coupure des câbles optiques sub-océaniques interrompra les communications et déconnectera les grands plateaux continentaux. La guerre pourra alors commencer.

Bruxelles, le 14 février 2014