WORKING PAPER

N°7 – 2007

NOUVELLES MENACES
NOUVELLES VULNERABILITES

Bouclier antimissiles (BAM) et Cyberwar

Academia Diplomatica Europaea

« PROMOTION SUN TZU »

5ème Année - 2007/2008

WORKING PAPER

N°7 – 2007

CONFERENCE

du mardi 11 Décembre 2007

de 18h00 à 20h00

NOUVELLES MENACES
NOUVELLES VULNERABILITES

Bouclier antimissiles (BAM) et Cyberwar

par

Irnerio SEMINATORE

Parlement Européen

Bâtiment Eastman – Salle 300 – 18:00-20:00

Rue Belliard 135, Bruxelles

INSCRIPTIONS

ACADEMIA DIPLOMATICA EUROPAEA

« PROMOTION SUN TZU »
« EUROASIAN GEOPOLITICS »

CINQUIÈME ANNEE

2007/2008

FORMATION POST-UNIVERSITAIRE

D'INITIATION
À LA REFLEXION GÉOPOLITIQUE, STRATÉGIQUE ET SYSTÉMIQUE
À LA PHILOSOPHIE DE LA GUERRE ET À LA SOCIOLOGIE DES CONFLITS
A LA SÉCURITÉ INTERNATIONALE
À L'ÉTUDE DE LA GLOBALISATION, DE LA COMMUNICATION ET DES MÉDIAS

MODULES D ENSEIGNEMENT

Le programme annuel sera réparti en cinq modules correspondant aux **cinq sections de l ADE** Ces dernières portent les noms des grands maîtres à penser, symbolisant les orientations doctrinales de l Académie.

« ***L Académie Stratégique - Carl von Clausewitz*** **»** à orientation stratégique, géopolitique et systémique;

« ***L Académie Diplomatique - Hugo Grotius*** **»** à orientation juridique, historique civilisationelle et de diplomatie publique;

« ***L Académie Economique - Ludwig von Mises et Friedrich von Hayek*** **»** à orientation économique, financière et praxéologique ;

« ***European War College - Johann von Neumann, Oskar Morgenstern et Wernher Von Braun*** **»** à orientation e-Intelligence, e-Politics, e-War et e-Space and Military Defense.

« ***L Académie de l'Information et de la Communication: Think-Tanks, Médias et Politique*** **»** à orientation information, communication, médias et aide à la décision.

En partenariat avec

FONDATION VINTU

POUR L EXCELLENCE DANS L ÉDUCATION ET LE JOURNALISME

PARLEMENT EUROPÉEN

DE BRUXELLES

BÂTIMENT EASTMAN SALLE 300

18-20 HEURES

ORGANISÉE PAR

L INSTITUT EUROPEEN DES RELATIONS INTERNATIONALES

INFORMATION

EMAIL : INFO@IERI.BE
SITE : WWW.IERI.BE
TEL : 02 280 14 95
ADRESSE : 27A BOULEVARD CHARLEMAGNE 1000 BRUXELLES

NOUVELLES MENACES,
NOUVELLES VULNÉRABILITÉS

Les nouvelles menaces, balistiques et cybernétiques.
Le bouclier anti-missiles (BAM) et le contexte global de sécurité

1. Introduction

Dans un environnement international caractérisé par un affaiblissement de l'Occident dans les grandes affaires du monde, deux séries de menaces, aux conséquences déséquilibrantes, sont à prendre en considération :

- **la première** est la menace balistique relançant la mise au point de systèmes antimissiles et, en retour, un abaissement du seuil de la dissuasion par une reprise de la course aux armements

- **la deuxième** est la menace informatique, préfigurant les cyber-conflits de demain, menace dont les aspects saillants sont d'attaquer les systèmes d information de l adversaire dans le but de :

- provoquer une intrusion dans leurs infrastructures, à caractère confidentiel ou classifié, afin de le pirater

- détruire les serveurs ennemis, de manière préventive ou en représaille

Eu égard à la première hypothèse, l Assemblée de l'UEO estime que le couplage des capacités nucléaires et des technologies relatives aux vecteurs balistiques, aux essais et performances perfectionnés en permanence, représente une des menaces les plus graves pour les équilibres stratégiques mondiaux et, en particuliers, pour un nombre croissant de pays européens du flanc sud, menaces venant d acteurs perturbateurs, dont les méthodes et les objectifs politico-stratégiques ne sont pas toujours prévisibles.

A cet égard les Etats-Unis mènent, depuis l initiative de défense stratégique (IDS) du Président Reagan, des recherches et des essais, visant à protéger le territoire des USA contre une attaque limitée de missiles adverses. Ce programme a été poursuivi par l Administration Clinton et est passé par des phases diverses, la National Missile Defense (NMD) puis le Missile Defense (MD) et aujourd hui la proposition d un bouclier anti-missiles (le troisième), avec un centre radar en Tchéquie et un centre d interception et d alerte avancée en Pologne.

2. Le contexte de sécurité

Du point de vue de la perspective, nous sommes sortis de la période messianique de l Europe et entrons dans une période où les retours de l espace et de la géopolitique mondiale, imposent à l UE, une nouvelle lecture de l avenir, celle de la « Balance of Power », théorisée par David Hume, et donc, à un choix d alliances à l échelle planétaire.

Le refus du messianisme a contraint à la découverte de nouveaux paradigmes structurants :

- l Eurasie à la place de l Europe
- l anarchie internationale au lieu de l intégration
- la définition des intérêts vitaux et donc une politique de sécurité et de défense pour des temps critiques

- le passage d une « logique de négociation permanente » entre Etats européens (dont les intérêts divergent) à une « logique proactive et unitaire », proposée par un leadership ou un directoire toujours refusés, dont la Commission demeure le passage obligé et le lieu d exercice privilégié.

- la prise en compte d un « agenda autonome » sur tous les problèmes internationaux, à partir de la « prolifération nucléaires à des fins pacifiques »

- la définition d une politique de défense anti-missiles et d options originales, en cas de négociations globales ou de marchandages multi-théâtres avec Moscou (Kosovo, Abkhazie, Transnistrie, Tchétchénie, etc.)

Immédiatement, le retour de la question russe, influe sur l'inversion de la question européenne. L élargissement de l OTAN abaisse-t-il le niveau de confiance mutuelle entre la Russie et l Alliance ? Le bouclier anti-missile permet-il de lier la « guerre longue au terrorisme » à la lutte contre la prolifération ?
A première vue, le bouclier anti-missile semble représenter un grignotage du Heartland russe.

Le premier paradigme, le passage du paradigme Europe à celui d Eurasie, concerne l UE et l OTAN. Il concerne non seulement la notion d espace géopolitique, mais aussi celui d Occident.
Depuis le 11 septembre 2001, la notion d Occident fait débat. Pour les américains, il y a désormais deux Occidents, un Occident européen et un Occident américain. Une divergence profonde les sépare en matière de rapports entre le droit, la force et l éthique.

Pour Moscou, la logique du double élargissement, celle de l OTAN (Pays Baltes, soutien aux révolutions de couleur à l instar de l Ukraine et la Géorgie) et celle de l Union européenne, remet en cause le leadership déjà périclitant de la Russie sur la Communauté des Etats Indépendants (CEI) et sur l étranger proche. D où l option de « décisions non négociées », retrait du Traité sur les forces

l intermédiaire «(TFI) et du « Traité sur les forces conventionnelles en Europe » (FCE), rééquilibrant l unilatéralisme des Etats-Unis.

En termes politiques, le bouclier anti-missiles (BAM) permet de gagner de l influence dans l Est européen. Poser la question des relations euro-atlantiques et le partage des responsabilités entre l Europe et les Etats-Unis, au moment du retour de la question russe et des incertitudes au Proche et au Moyen-Orient, signifie stopper la dérive ou les glissements stratégiques américains vers l Asie.
Avant d aborder le thème des relations euro-atlantiques, une question domine les relations infra-européennes, la question russe, et celle-ci peut être formulée ainsi :
« La Russie est-elle un rival ou un partenaire stratégique ?

Cette question se double par ailleurs des options sur les garanties de sécurité. En effet tout le flanc sud de l Alliance est à la portée des missiles de théâtre en provenance de l Iran. Le BAM pose de multiples dilemmes, dont celui, technique, des systèmes de défense intégrés, qui fragilisent les forces nucléaires européennes autonomes (françaises et britanniques) et remettent en cause la défense européenne.

De plus, il risque de provoquer une division politique au sein de l Alliance et, en son fond, remet en cause tous les traités de sécurité euro-atlantiques existants. La nouveauté est représentée par le fait que les Etats-Unis refusent le vieux concept de MAD et donc la possibilité d une première frappe imparable. Le BAM tient compte de l évolution des réalités de la puissance et donc de lapossibilité de porter le danger et la menace chez les autres. Il pose en son fond la résurgence des fondamentaux de la puissance.

La défense anti-missile s applique à l interception et à la destruction de vecteurs de très longue portée et douées d une vitesse supérieure à l ensemble des autres armes aériennes, appartenant à des

générations de conception ancienne et rustique, ou à des engins récents et sophistiqués. Contre ce type d arme, aux capacités de pénétration sans équivalent, l efficacité de la défense exige des moyens, des principes et des architectures de protection qui suscitent débat, affirmations et perceptions contradictoires, voire affrontements interétatiques et géopolitiques. La défense anti-missile est par ailleurs susceptible d induire des altérations dans les grands équilibres stratégiques du continent européen, et de bouleverser les démarches entreprises au sein de l OTAN, au Sommet de Riga de décembre 2006, concernant les implications politico-militaires de cette éventuelle défense anti-missile avancée. L évolution récente de ces systèmes de défense, par l abaissement du seuil de parité entre attaquant et défenseur et la prime assurée à l attaquant, risque de rendre obsolète la dimension codifiée par le MAD (destruction mutuelle assurée). Dans ce contexte elle lèse un principe discriminant et intangible : la non identité des intérêts de défense entre l Europe et les Etats-Unis.

3. La menace cybernétique

La deuxième source de menaces et donc de vulnérabilités est la guerre électronique. Le leader incontesté dans ce type d exercice est la Chine. Cent-soixante millions d utilisateurs, strictement contrôlés par l Etat utilisent Internet, dont le régime se sert comme outil de propagande, d information et de désinformation. Depuis 2000, l'Hackers Union of China échange des tirs groupés contre d autres groupes ou cibles étrangers. Dans ce cas, comme dans beaucoup d autres, il n y a pas de pratique sans théorie, ni de théorie sans doctrine. En effet, l analyse des nouvelles formes d actions offensives dans le domaine des guerres de demain est la résultante d une intéressante étude chinoise : « La guerre hors limite ». Dès lors, on peut imaginer des scénarios de conflits à plusieurs dimensions.

4. Cyberguerre et menace informatique.

Guerres hypothétiques et hyperboliques.

Au seuil de la prochaine guerre mondiale, trois types de menaces se transformeront en attaques immédiates, simultanées et préventives :

- les menaces cybernétiques
- balistico-satellitaires et terroristes
- les attaques climatiques, volcaniques et sous marines, par la pose de bombes atomiques d activation sismique.

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

La guerre pourra alors commencer.

Ainsi, le contexte mondial dans lequel s inscrira toute attaque de grande ampleur, conjuguera les antagonismes rationnels des Etats, les rivalités hégémoniques des acteurs majeures de la globalisation, les actions de représailles et les stratégies géopolitiques mises en S uvre par les services électroniques et d espionnage, une compétition économique acharnée, et de formes renouvelées de mésententes idéologiques, mêlées à des actes de piraterie patriotiques.

Des « chocs des civilisations », traditionnels ou extrémistes, doublés de nouveaux conflits urbains, intracommunautaires et ethniques, s ajouteront à ces scénarios hyperboliques.

A la lumière de ces hypothèses, les menaces apparaitront pour ce qu elles sont : des conflits non déclarés et des dangers immanents, à potentiel de létalité élevée. La « menace informatique » y jouera

un rôle « soft » et impalpable, comme aveu implicite d une paralysie, toujours possible, des rythmes effrénées 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 ».

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

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

- l identification préalable des secteurs clés, civiles 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 avancés et de secteurs de production des ordinateurs

Le principe capital de la menace, puis de l attaque informatique, repose sur sa forme résolument offensive, coordonnée et directe. La première règle 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, la pratique étendue et l utilisation stratégique de l « intelligence » et de l espionnage, civil et militaire, l orchestration et la mobilisation collective de toutes les ressources

humaines disponibles, le culte de l héroïsme et des valeurs martiales à des buts individuels de recrutement et d emploi offensif et à des fins collectifs de dominance cybernétique. Du côté des adversaires (Occident), l absence de réflexes d autodéfense et les faux calculs économiques et diplomatiques, la dégradation rapide des conditions de l autodéfense informatique, européenne et occidentale, 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, des puissances adverses, résulte d un constat patent et d une série d actes offensifs, ayant touchés plusieurs pays occidentaux (Estonie, Allemagne, France, Etats-Unis, Japon, Nouvelle-Zélande, etc.). Ces avertissements et formes d attaques diverses on testé et démontré des formes de vulnérabilités nouvelles des infrastructures et des réseaux informatiques occidentaux. En effet, une nouvelle forme de conflit vient de naître, depuis une dizaine d année, la **guerre d information électronique** ou « **cyberguerre** », théorisée et codifiée, travaillant 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 de frapper et d incapaciter totalement l adversaire.

Irnerio SEMINATORE

Bruxelles, janvier 2008