L'infosphère Composante opérationnelle émergente, enjeu majeur pour le traitement des crises futures. Sphère informationnelle et guerre de l'information
août 2006

La révolution des NTIC, corollaire du phénomène actuel de mondialisation, a transformé notre environnement en une véritable "société de l'information" où la téléphonie mobile, l'Internet, la numérisation de l'image constituent un maillage formant une vaste enveloppe immatérielle appelée infosphère. La course aux armements s'est doublée d'une course à la technologie de l'information et de la communication. Comprendre l'infosphère et en saisir les enjeux, c'est tenter d'analyser le concept et réfléchir à cette question : en quoi est-il indispensable pour l'avenir de parvenir à la maîtriser ? (Maîtrise par la technique mais aussi par l'adaptation de nos systèmes de pensée aux "guerres de la troisième vague" (L. Francart).

De la guerre électronique à la guerre de l'information

Le néologisme "guerre de l'information" apparaît au début des années 90, dans les rapports officiels et la littérature spécialisée, accompagné d'autres mots comme "infoguerre", "cyberguerre", "dominance informationnelle", ou encore "guerre cognitive" (C.Harbulot), et plus récemment "maitrise de l'information" qui s'impose à la fin des années 90 (L.Francart). Cette notion n'est pourtant pas clairement définie et la vogue de la guerre de l'information "s'accompagne d'une grande imprécision de son contenu exact" (H.Coutau-Bégarie).

En 1995, Martin Libicki, professeur à la *National Defense University*, soulignait déjà le côté nébuleux du concept dans son ouvrage *What is information Warfare ?* On peut dire cependant que la guerre de l'information s'inscrit dans la continuité de la guerre électronique qui remonte à des dizaines d'années, et dont la doctrine et les systèmes sont éprouvés.

Certains théoriciens voient dans le seul domaine physique le caractère essentiel de la guerre de l'information ("un conflit électronique dans lequel l'information est une valeur stratégique, méritant conquêtes et destructions" pour l'américain Winn Schwartau, inlassable prophète d'un "Electronic Pearl Harbor"). Cette théorie est vivace et les rapports catastrophistes sur les cyberterroristes, les mises en garde contre une attaque généralisée des systèmes : bourse, transports, banques, énergie… et autres constats alarmants ne manquent pas. Pourtant, mener à bien une action coordonnée à l'échelle d'un pays et dans un laps de temps très limité serait d'une grande difficulté. Bien que des actes interétatiques de piratage informatique aient déjà eu lieu, les dommages furent jusqu'à présent essentiellement symboliques (exemples des "hacktivistes" serbes contre l'ordinateur central de l'Otan, du Timor oriental contre l'Indonésie, de la Chine contre Taïwan…).

Cependant, la dimension psychologique ne saurait être exclue de la guerre de l'information. La notion de guerre psychologique reparaît en France dans les années 90, lorsque la nécessité s'en fait ressentir dans les Balkans, pour la première fois depuis les événements d'Algérie (les opérations psychologiques furent bannies après la perturbation politique et le traumatisme qui suivirent l'épisode des 5èmes bureaux).

La guerre psychologique consiste généralement à lancer des opérations qui visent à attaquer soit le moral, soit les croyances d'un adversaire, de ses dirigeants, de sa population et de ses alliés et, en même temps à protéger sa propre population, ses dirigeants et ses alliés contre les actions de guerre psychologique de l'adversaire. Ainsi la "*Voice of America*" fût un outil de guerre psychologique très efficace au cours de la guerre froide, quand la dissuasion nucléaire mutuelle laissait le terrain aux manœuvres indirectes…

Vers la maîtrise de l'information ?

Pour le *Department Of Defense* américain (*DOD*) la guerre de l'information est "l'ensemble des actions entreprises pour atteindre la supériorité dans l'information en affectant l'information, les processus informationnels, les systèmes d'information et les réseaux informatiques de l'adversaire, tout en défendant sa propre information, ses propres processus informationnels, systèmes d'information et réseaux informatiques". Une fois la domination de l'information atteinte, la guerre de l'information serait gagnée. Tel est le concept de la *Revolution in Military Affairs* (*RMA*). Né des groupes de travaux américains, ce mot qui s'impose à partir de 1994 dans la littérature universitaire et militaire, se réfère à un rapport précédemment établi devant tirer les enseignements de la guerre du Golfe, qui pointait l'utilisation décisive de la gestion électronique de l'information et de la logistique, de l'observation satellitaire et des armes de haute précision (guidage laser), dans le chapitre : "révolution militaire".

L'idée d'une révolution militaire impulsée par les NTIC n'est pas nouvelle : fin des années 70, les Soviétiques avaient déjà forgé le terme : "révolution techno-militaire" pointant le rôle fondamental des machines informatiques, la détection spatiale et les systèmes balistiques électroniques et à grande portée dans la conduite des guerres. Dans l'optique américaine, la supériorité informationnelle absolue doit être atteinte et conservée, elle devient un objectif stratégique de premier ordre.

Ce concept comporte néanmoins des failles importantes, comme les difficultés inhérentes au traitement de l'information : l'exemple du 11 septembre montre que la *NSA*, la *CIA* et le *FBI* possédaient des informations parcellaires qui auraient dû alarmer ces instances si elles avaient été croisées. La collecte d'informations ne suffit pas, la fusion du renseignement est nécessaire pour prévenir les menaces.

Plus qu'un concept établi, la *RMA* doit être perçue comme un "mot-programme", une nouvelle arme de dissuasion américaine, qui vise à rendre inconcevable pour l'adversaire l'idée d'une agression anti-américaine.

Pour l'Europe la stratégie est différente : l'objectif fondamental, en matière de sécurité et de défense, est l'acquisition d'une capacité d'anticipation et d'aide à la maîtrise des situations de crises, et ceci par la maîtrise de l'information, non pas sur l'ensemble du spectre ("*full spectrum dominance*"), mais dans les domaines qui facilitent l'atteinte du but visé.

En France, l'armée de l'air réalise un travail précieux au sein de l'infosphère de défense (exemple de l'AWACS).

La conception d'une stratégie de défense efficace nécessite l'intercommunication des réseaux politiques, économiques et militaires. Dans ce sens la commission européenne a lancé le projet de création d'une "*cyber security task force*".

Si la "maîtrise de l'information peut paraître utopique", l'expérience de la guerre électronique peut faire progresser plus rapidement la terminologie, la doctrine et les systèmes dans un contexte de guerre des réseaux informatiques.

L'infosphère –
Composante opérationnelle émergente, enjeu majeur pour le traitement des crises futures août 2006

La numérisation du champ de bataille, dimension opérationnelle de l'infosphère

La maîtrise de l'information sur le champ de bataille

L'objectif pour les Européens n'est pas d'acquérir la supériorité dans le domaine de l'information, à l'instar du concept américain *information dominance* (l'écart de moyens entre eux et nous est trop important), mais de maîtriser l'information sur une bande passante utile à la réalisation de la mission. Autrement dit, il s'agit de mettre en œuvre une "infostratégie" pour disposer de l'information nécessaire à la planification et à la conduite des opérations.

Le cycle de l'information comprend en premier lieu le recueil de l'information, puis l'analyse de l'information et sa synthèse en vue d'améliorer la connaissance, et au final la prise de décision.

Une fois recueillie (par des capteurs : exemple du réseau américain *échelon)*, l'information est numérisée pour être exploitée le plus rapidement possible. Il faut introduire des filtres efficaces pour ne garder que l'information utile à la décision. La recherche consiste à actualiser, de façon permanente et en temps réel, la connaissance acquise pour permettre ainsi l'obtention d'une"longueur d'avance" sur l'adversaire.Le processus de transmission de l'information comprend un émetteur qui communique l'information, un vecteur c'est-à-dire la voie par laquelle la communication est transmise, et un récepteur ou cible à qui est destinée l'information. Le vecteur peut être le lieu d'interception d'informations, en particulier de celles transmises par voie électrique ou électronique (écoute des émissions hertziennes, pénétration des réseaux informatiques, en particulier avec Internet… pour s'emparer de l'information et éventuellement de la transformer)

Le concept américain de guerre de réseau *network centric warfare* transforme la supériorité de l'information en avantage stratégique sur le champ de bataille. Tous les organes de commandement sont entièrement basés sur les technologies de l'information (TI) : ordinateurs, systèmes de communication complexes… Les organismes militaires et civils dépendent beaucoup des TI, ce qui crée des failles nouvelles exploitables lors d'un conflit, d'où le concept de guerre de l'information (voir la fiche : guerre de l'information). La supériorité de l'information sur le champ de bataille est le résultat des opérations qui ont réussi : l'information circule librement entre les forces amies mais l'ennemi en est privé.

Les Systèmes d'Information Tactique (SIT), outils de la guerre moderne.

Ils ont un rôle crucial sur le champ de bataille en indiquant la localisation exacte des troupes amies et adverses (par exemple à l'aide des cartes de situation géographique numérisées). Le système américain *Force XXI Battle Command, Brigad and Below* (FBCB2) a la capacité de transmettre les positions et d'assurer les communications entre les engins mais aussi de générer au niveau des véhicules des rapports de situation logistique (état des munitions, du carburant…) et humains (morts, blessés).

Puissant outil dans la chaîne de commandement, les SIT sont néanmoins un outil coûteux, ils nécessitent des développements longs et continus en matière de recherche d'une part (exemple américain du *rehearsal* : simulation avant le combat), qui peuvent déboucher sur de très rentables applications commerciales, et en matière de dépendance stratégique d'autre part (lorsque ces systèmes tournent sur base de logiciels dont tous les codes source ne sont pas à disposition des armées qui les utilisent : exemple de Windows). La numérisation de l'espace de bataille (NEB) est prévue pour l'ensemble des forces françaises à l'horizon 2012-2015. Ces systèmes permettent de diminuer drastiquement le taux de tirs fratricides, ils optimisent l'économie des forces et la précision des feux

(comme l'ont illustré les opérations en Irak). La transmission satellitaire constitue un élément-clé du dispositif.

Mais ils présentent également des inconvénients d'ordre technique et humain :

- Ils peuvent être saturés : en Irak et en Afghanistan, plusieurs commandants achetaient eux-mêmes des téléphones satellites pour dépasser les lenteurs du système et atteindre leurs supérieurs.

- Si le système ralentit pour cause d'attaques contre des relais (opérations "techno-asymétriques") ou encombrement de la bande passante, il n'accélère ni ne sécurise plus le combat mais au contraire, le ralentit et le rend plus dangereux en donnant des informations dépassées.

- Les SIC (niveau supérieur de commandement) français de l'Armée de Terre ont une interopérabilité insuffisante sur le champ de bataille parce qu'ils sont développés par différentes entreprises industrielles dont les contraintes et les besoins divergent.

- L'enlisement irakien montre que si ces systèmes s'avèrent être de fabuleux outils opérationnels, ils ne constituent pas une solution miracle. Ils ne peuvent prendre en compte ni l'état du moral des troupes ni la fatigue des hommes.

Le développement des programmes spatiaux militaires, **enjeu majeur pour la Défense**.

Les moyens satellitaires affranchissent des masques du terrain et donnent une capacité d'anticipation dans l'action, ils confèrent ainsi un ascendant sur l'adversaire comme sur les partenaires. Ils contribuent à l'évaluation d'une menace, au suivi des évènements dès les prémices d'une crise, et aux travaux de planification.

Hormis les Etats-Unis qui combinent un quasi-monopole de la couverture satellitaire et la maîtrise d'Internet et surtout de ses logiciels d'accès, les modes de transmission de l'information échappent aujourd'hui largement aux puissances, qui n'ont pas su se doter des moyens techniques nécessaires.

Or les transmissions satellitaires rendent certains pays dépendants des Etats régisseurs : un Etat propriétaire du satellite peut retarder la disponibilité de l'information par "blocage" de la liaison satellite.

L'obtention à terme d'une couverture satellitaire totale est un enjeu majeur de souveraineté pour la France.

Dans une dimension européenne, les programmes spatiaux s'inscrivent dans une volonté de partage avec nos alliés (système "Helios"). Une large autonomie dans l'espace s'avère être indispensable pour la future Europe de la Défense.

Parce que tous les systèmes d'armes futurs utiliseront massivement des composantes électroniques et des logiciels élaborés, et qu'en définitive les systèmes électroniques multiplient l'efficacité des armées, bien qu'ils soient en contrepartie la source de nouvelles vulnérabilités.