

La guerre de l'information, guerre du XXI^e siècle

La guerre de l'information n'est pas un concept récent mais aussi classique que l'art de la guerre lui-même. Il existe donc un parallèle entre les principes qui ont gouverné les anciennes formes de conflits et les nouveaux aspects d'une confrontation basée sur l'information et sa circulation. Les concepts traditionnels sont ceux donnés par Sun Tzu dans *L'art de la guerre*. Ces concepts sont, par conséquent, à réactualiser suite aux récentes avancées technologiques des systèmes d'information et de communication (SIC) qui véhiculent de nouvelles menaces pour notre sécurité nationale et notre économie.

Une définition

La définition donnée de l'*Infowar* (IW) est la suivante : interdire à l'ennemi la capacité à mener la guerre en lui ôtant sa volonté et sa capacité à lutter contre vous par une maîtrise de l'information.

La guerre de l'information est une problématique qui doit s'adresser aux décideurs de façon générale, qu'ils soient politiques, économiques ou militaires. Elle pose les enjeux des nouvelles formes que prend la guerre via les nouvelles technologies précitées.

Par l'interconnexion même des systèmes d'information, il est difficile de discriminer la menace en fonction des niveaux politico-militaire, opératif ou tactique. La numérisation de nos sociétés touche aussi nos organes de sécurité et met en relation quasi-instantanément tous les niveaux de décisions. En somme, une menace à un niveau est directement une menace pour l'ensemble ce qui permet de tirer des enseignements pour notre Défense de façon générale.

Dans ce cadre, il est urgent de faire prendre conscience de l'acuité et de la nocivité de cette menace insidieuse qui relève de la stratégie indirecte théorisée par Sun Tzu mais aussi Liddell Hart. L'objectif est d'empêcher l'adversaire de coordonner sa défense, de semer la confusion, de diminuer sa capacité et sa volonté de résistance, de désorganiser la vie du pays. Il s'agit de vaincre l'adversaire avant même d'engager des moyens directs qui n'auront plus qu'à cueillir un fruit mûr.

Loin d'être virtuelles, les menaces issues des nouvelles technologies de l'information sont d'ores et déjà bien réelles. L'attaque massive des systèmes d'information publics estoniens par la Russie en mai 2007 est un exemple. La Défense nationale et les organes gouvernementaux furent la cible d'attaques en déni de service par le biais de plusieurs réseaux étrangers. Serveurs, éléments actifs des réseaux des fournisseurs d'accès et des banques du pays n'ont pas été épargnés. Les attaques n'ont cessé qu'au bout de 3 semaines. Un écho (*ping*) a été envoyé vers des serveurs qui, en répondant, ont été infectés. Au bilan : 300.000 serveurs touchés en moins d'un quart d'heure. La simplicité de l'attaque met alors à jour la faiblesse des défenses en la matière. On peut citer également l'attaque du réseau français Intradéfense en 2007 ou du réseau militaire américain NIPR en 2008 avec, cette fois, la Chine pour pays fortement soupçonné.

Pourtant des contre-mesures existent bel et bien

En France, le gouvernement a décidé de passer en matière de sécurité des réseaux d'une posture défensive à une position agressive. Résultat d'arbitrages entre les professionnels du secteur et le Conseil de défense, le Livre blanc, présenté au président de la République, aborde cette problématique. *"Face aux attaques informatiques, j'ai décidé de doter pour la première fois la France de capacités défensives et offensives qui concerneront aussi bien toutes les administrations que les services spécialisés et les armées"*, a déclaré Nicolas Sarkozy devant un parterre de militaires.

La prise de conscience du politique semble forte : la guerre informatique, dont les acteurs vont des "hackers" aux États en passant par les groupes terroristes et mafieux, *"est devenue une réalité"*. *"Dans le domaine informatique plus que dans tout autre milieu il faudra, pour se défendre, savoir attaquer"*, lit-on dans cet ouvrage qui fixe les grands axes de la politique de défense de la France pour les 15 prochaines années. *"// convient donc de disposer d'une capacité de neutralisation à l'intérieur même des centres d'opérations adverses"*, ajoutent les auteurs de ce document.

Le Livre blanc recommande également le développement d'outils spécialisés ("armes numériques de réseaux", "laboratoire technico-opérationnel" ...), la définition d'une doctrine et d'un cadre d'emploi de ces moyens et la formation de personnels. Le cadre d'emploi *"devra respecter le principe de riposte proportionnelle à l'attaque, visant en priorité les moyens opérationnels de l'adversaire"*, stipule-t-il cependant. L'internationalisation des mesures est également mise en avant. *"Il serait illusoire de limiter la lutte contre la cybercriminalité au seul cadre national"*, expliquait lors des Assises du Numérique, la ministre de l'Intérieur, Michèle Alliot-Marie.

En matière défensive, le Livre blanc prévoit la création, à l'image de la *Computer Emergency Readiness Team* (CERT) américaine, d'une *"agence de la sécurité des systèmes d'information"* dont la tâche sera de

détecter les attaques informatiques et d'y réagir, grâce à un centre chargé de surveiller les réseaux "sensibles". Cette agence sera également chargée de la prévention et devra contribuer au développement d'une offre industrielle de matériels de très haute sécurité pour la protection des secrets de l'État, des administrations et des acteurs économiques. Elle devra en outre informer régulièrement le public sur les menaces informatiques. Elle sera mise en place à partir de la Direction centrale de la sécurité des systèmes d'information créée en 2001, où travaillent 110 personnes.

Pour se donner les moyens d'une telle politique, le budget affecté à cette fonction va doubler, pour passer de 350 à 700 millions d'euros par an.

Le politique a pris en compte cette menace. Il faut maintenant que les armées soient motrices si elles veulent rester centrales dans les problématiques de Sécurité nationale.

En amont, elles doivent s'impliquer davantage dans l'élaboration des postures défensives et offensives de la guerre de l'information via la Délégation Générale des SIC (DGSIC), le Centre Interarmées de Concepts de Doctrines et d'Expérimentations (CICDE), le Centre de Doctrine et d'Emploi des Forces (CDEF), la Délégation Générale pour l'Armement (DGA à travers le Celar) et les autres centres de recherche de la défense comme celui de l'Ecole Supérieure et d'Application des Transmissions (ESAT) mené par le lieutenant-colonel Eric Filiol, expert internationalement reconnu en la matière.

En aval, la protection physique et logique des Postes de Commandement (PC) doit être renforcée. Tous ceux qui ont approché de près les Centre Opérations (CO) de nos brigades ou divisions ont été témoins de l'instabilité du réseau de commandement opérationnel SICF (Système d'Information et de Commandement des Forces) en environnement Windows, fait accentué par des architectures et des versions évoluant à chaque exercice. Les administrateurs ne peuvent donc maîtriser le cœur de l'outil en faisant du *drill* comme les autres fonctions opérationnelles. A chaque exercice, les Transmetteurs effectuent de la « découverte opérationnelle » et sont donc incapables de résoudre rapidement un dysfonctionnement majeur sans l'appui de l'industriel (Thalès). Imaginons un blocage du système d'information (pour cause d'instabilité, d'intrusion de virus voire d'Impulsion Electro Magnétique (IEM)) en pleine phase de coercition terrestre avec impossibilité d'un retour rapide en mode nominal faute d'une connaissance profonde du système. Ce scénario catastrophe s'est déjà produit, fort heureusement à l'entraînement : en 1998, le navire américain *USS Yorktown* fut paralysé à cause du blocage de ses systèmes d'information suite à l'introduction d'un applicatif militaire dans un environnement Windows NT.

Cet état de fait doit nous inciter à l'humilité en imposant des entraînements réguliers de nos PC opératifs en mode dégradé, « à l'ancienne », avec phonie, graphie et cartes papier afin de rétablir le plus rapidement possible le commandement d'une grande unité et ne pas subir la guerre de l'information comme une nouvelle *blitzkrieg*...

Les hautes sphères Outre-Atlantique, dont celles de la Défense, se penchaient déjà il y a dix ans sur cette problématique. La France se doit de réagir. Si le politique vient d'opter pour une action volontariste, il faut que les armées se réapproprient cette partie de la guerre un peu iconoclaste pour des officiers encore essentiellement imbibés de ses aspects clausewitziens.

Patrice HUIBAN

