Cyberconflictualité et forces terrestres : y a-t-il une spécificité du milieu ?

Synthèse de la journée Cyber-conflictualité et forces terrestres, Rennes, 12 février 2013

Gérard de Boisboissel & Didier Danet
CREC Saint-Cyr, Pôle Action globale et forces terrestres

Mai 2013. Article n°5.1

L'une des particularités les plus fréquemment mises en avant de la cyberconflictualité serait l'existence d'un continuum de la menace, les mêmes agresseurs pouvant se servir des mêmes instruments pour mener des actions hostiles à l'encontre de n'importe quel acteur civil ou militaire selon des modes opératoires uniformes. Aucune frontière ne pourrait être tracée au sein du cyberespace entre les acteurs, les domaines d'intervention, les modes d'action... Il en résulterait une nécessaire globalité de la réponse des pouvoirs publics qui, tant sur le fond des politiques à adopter que dans l'organisation institutionnelle de la cyber-défense, devrait ainsi être «tout inter» : inter-armées, interministérielle, civilo-militaire, internationale.

L'hypothèse d'un cyber-espace totalement décloisonné et dans lequel la menace serait susceptible de se déployer uniformément et sans être influencée de quelque manière que ce soit par les traits particuliers du milieu local apparaît cependant quelque peu audacieuse. Même si le principe de la menace est globalement le même (porter atteinte à l'action d'un ensemble d'organismes civils ou militaires par la dégradation de leurs systèmes interconnectés), ses conditions de mise en œuvre, ses effets potentiels et les ripostes susceptibles de lui être opposées différeront sans doute sur de nombreux points, certains marginaux, d'autres plus essentiels. Pour s'en tenir au seul domaine de la cyber-menace à l'encontre des forces armées, les caractéristiques du cyber-espace de l'armée de Terre ne sont certainement pas identiques à celles de la Marine ou de l'armée de l'Air. Par nature, l'armée de Terre est déployée dans un espace géographiquement étendu, peu prédictible, hétérogène, plus ou moins cloisonné, où ses différentes unités sont dispersées et où l'interconnexion filaire, par exemple, n'a guère de sens. Les Forces terrestres opèrent en outre souvent au cœur

des populations, induisant une vulnérabilité plus grande aux actions hostiles sur les infrastructures de communication de proximité, ainsi qu'un risque plus élevé de soulèvement de foules de plus en plus interconnectées au travers des réseaux sociaux, où l'information n'est pas facilement contrôlée, ni sa diffusion maîtrisable. Le milieu est évidemment tout autre pour un bâtiment de la Marine ou une escadrille de chasse.

La question se pose donc légitimement d'une réflexion qui ne soit pas d'emblée située au plus haut niveau «inter» et qui prenne en compte les caractéristiques particulières de chacun des milieux considérés : celui des entreprises ou des administrations, celui des forces terrestres, maritimes ou aériennes... En quoi les caractères particuliers des organismes, des dispositifs de traitement numérisé de l'information et des interconnexions qui constituent le cyberespace influencent-ils les figures de la cyberconflictualité ? Dans quelle mesure les caractéristiques du milieu physique dans lequel intervient l'entité interconnectée sont-elles susceptibles de donner naissance à des formes spécifiques de cyberconflictualité ? Les menaces doivent-elles appréhendées de manière globale ou faut-il les envisager de manière différenciée selon le milieu local dans lequel elles sont susceptibles de se produire ? Le bon niveau d'organisation de la cyberconflictualité est-il nécessairement le plus élevé dans la dimension «inter» ? Les réponses à apporter aux cybermenaces seront-elles d'autant plus efficaces qu'elles présenteront un caractère universel ?

La journée organisée par le pôle Action Globale et Forces Terrestres des Ecoles de Saint-Cyr Coëtquidan avait précisément pour ambition de dresser un état des lieux de la cyberconflictualité envisagée sous l'angle des particularités du milieu dans lequel agissent les forces terrestres. Cette journée appelle bien évidemment un prolongement d'une part pour poursuivre l'exploitation méthodique des particularités du milieu terrestre et, d'autre part, afin de comparer les résultats obtenus avec ceux dégagés par la Marine et l'armée de l'Air.

De cette journée de réflexion se dégage une première conclusion relative à la nécessité de préparer l'ensemble des forces, et non pas les seuls spécialistes, à la question de la cyberconflictualité. Mais, une sensibilisation générale des personnels de l'armée de Terre aux enjeux et aux formes de cette cyberconflictualité suppose de développer des modules de formation adaptés, qui ne soient pas rendus hermétiques par une approche trop exclusivement technique et reposant sur des prérequis importants en matière de systèmes d'information. Trois couches de formation peuvent être envisagées. La première viserait à acculturer

l'ensemble des personnels à la cyberdéfense et constituerait un «fond de sac» devant être connu de tous. Elle pourrait donner lieu à des exercices permettant de vérifier l'acquisition par les personnels des réflexes nécessaires en cas de cyberattaque. La deuxième correspondrait à un premier niveau de compétence technique permettant aux personnels formés d'assurer la défense des réseaux existants. La troisième se situerait à un niveau d'expertise sans que le positionnement précis de ces experts dans le dispositif ne soit aujourd'hui nettement défini. Se pose en particulier la question de la cyber-réserve citoyenne qui pourrait être constituée afin de fournir aux forces armées une expertise constamment au fait de l'évolution des menaces et des techniques de protection ou de lutte contre les cyber-attaques. La cyber-réserve citoyenne constituerait une alternative budgétairement avantageuse et garantissant un haut niveau d'expertise dans les domaines considérés.

Une question générale se pose sur la nature et l'ampleur des changements à apporter à l'organisation actuelle des forces du fait du développement de la dimension cyber de la conflictualité contemporaine. Dans de nombreux pays, des chaînes de commandement cyber ont été mises en place ce qui complique l'organisation existante. En particulier, la question de la création d'un cybercommandement spécifique se pose au regard notamment de l'existence de l'arme des Transmissions, arme ancienne et qui dispose d'une incontestable compétence en matière de guerre électronique aussi bien que de protection des réseaux. En pratique, l'action globale des forces terrestres impliquera nécessairement une dimension cyber en préparation de la mission et dans sa mise en oeuvre sur le terrain. Chaque régiment devra être préparé à la mise en œuvre de la cyber-conflictualité, notamment dans sa dimension de protection des équipements numériques et des systèmes de traitement de l'information, la fonction d'expertise et d'action spécifiques revenant à des unités spécialisées de l'armée de Terre et/ou inter-armées. L'irruption du cyber-espace implique-t-il la création d'une nouvelle chaîne de commandement ? Dans l'affirmative, ne risque-t-elle de provoquer le morcellement de l'autorité décisionnelle et de priver les responsables sur le terrain des effets positifs associés au principe de subsidiarité ?

Tout effort consenti en faveur de la cyberconflictualité se faisant à effectif constant, il convient de mesurer précisément le coût économique de la priorité qui est susceptible de lui être accordée en prenant en compte les sacrifices qui devront être opérés sur les ressources allouées aux autres fonctions opérationnelles. Accroître la capacité de résilience des systèmes militaires et de ceux qui les servent apparaît comme un objectif souhaitable. Pour autant, cette

prise en compte de la résilience dans le fonctionnement des dispositifs militaires suppose l'acceptation d'un surcoût au niveau de la formation des personnels et, également, de la sécurisation des systèmes pour qu'ils puissent fonctionner en mode dégradé. La question du mode de fonctionnement dégradé soulève d'ailleurs une interrogation sur sa pertinence et sa faisabilité. Est-il possible d'imaginer un double niveau de formation qui ferait intervenir de manière systématique le mode normal de fonctionnement des systèmes numériques et un mode plus ou moins dégradé ? La question se pose en particulier au monde militaire qui ne saurait admettre la paralysie de son action et de ses systèmes d'armement du fait d'une cyber-attaque ou de toute autre cause d'interruption de ses composantes numériques (panne, manoeuvre de guerre électronique, bug informatique...)

La question du coût de ces mesures de protection doit être rapportée au fait que la cyber-menace pèse sur l'ensemble des dispositifs civils et militaires, ces derniers ne pouvant être considérés comme spécifiques et totalement protégés du fait de leur relative indépendance à l'égard des réseaux numérisés conventionnels. Mais, d'une part, les systèmes militaires sont dotés en plus ou moins grande partie de composants issus du monde civil et, d'autre part, l'indépendance de ces réseaux n'atteignant que très exceptionnellement le degré d'une totale étanchéité (opérations de maintenance par exemple), la mise en place de mesures de protection est indispensable pour se garder d'un illusoire sentiment de sécurité.

La doctrine d'emploi de la cyberdéfense soulève des interrogations pratiques aussi bien que théoriques. Il est généralement admis que le manque de maîtrise des effets d'une cyberattaque conduit les pays comme la France à ne pas envisager de s'en faire les auteurs et à concentrer les efforts sur la protection des systèmes, la lutte informatique défensive. Mais, ce principe une fois affirmé de manière assez générale, la délimitation des frontières entre cyberattaque et cyberdéfense n'est pas sans poser un certain nombre de difficultés. Par exemple, faut-il limiter la défense d'un système à la neutralisation de la cybermenace ou celle-ci autorise-t-elle à riposter à la cyberattaque en agressant l'auteur et/ou le vecteur de cette attaque ? Faut-il aller plus loin et envisager des attaques préventives contre des systèmes ennemis potentiels ou avérés ? De la même façon, la cyberdéfense ne peut se concevoir isolément et elle doit être articulée avec les domaines qui lui sont connexes ou complémentaires (guerre électronique, information et désinformation...)

Cette journée nous permet de constater l'intérêt d'une réflexion par milieu, complémentaire de l'analyse qui a traditionnellement cours et qui envisage la cyber-conflictualité sous ses aspects inter-ministériels et inter-armées. Elle soulève de nombreuses questions théoriques et pratiques en ce qui concerne l'organisation de la cyber-défense, sa doctrine, sa mise en œuvre au sein des forces, la formation des personnels... Le pôle Action globale et forces terrestres se propose en conséquence de poursuivre cette réflexion. Il organisera en particulier en juin et au cours de l'automne une série de colloques ouverts à tous. En tant que de besoin, il reconduira des journées d'études orientées vers le public spécialisé des forces.