Sécurité et conflits au XXIe siècle

Philippe Baumard

Cyberwar: Security, Strategy and Conflict in the Information Age

Fairfax, Virginie: AFCEA, 1996

Alan D. Campen, Douglas Dearth, Thomas Goodden (Eds.)

Citation : Ph. Baumard (1997), « Sécurité et conflits au XXIe siècle » commentaire de l'ouvrage d'Al Campen (ed.), Cyberwar: Security and Conflict in the Information Age, Fairfax, *Revue Française de Géoéconomie*, Vol 1 ; No 2, 1997.

Cet ouvrage publié par l'*Armed Forces Communications and Electronics Association*, appartient à une série de publications sur les sciences du commandement et l'utilisation des technologies de l'information dans les secteurs civils et militaires aux États-Unis. Dirigé par des enseignants de la *School of Information Warfare and Strategy* de l'Université de Défense Nationale américaine, et de l'Army War College, il regroupe vingt-trois contributions d'experts de la « guerre de l'information », incluant Martin Libicki,Daniel Kuehl et Thomas Rona.

L'ouvrage est divisé en quatre parties. Une première série de contributions examine la lente révolution que fut celle de l'utilisation d'information avancée dans les conflits militaires et la domination géoéconomique. Les concepts traditionnels de la puissance y sont sérieusement remis en cause. La discontinuité, le caractère imprévu et la nature civile et criminelle des nouvelles menaces appellent une réorganisation de la défense nord-américaine autour d'une capacité nationale de guerre de l'information. Réalistes, Dearth et Williamson (pp. 13-29) concèdent qu'une partie de la population mondiale devra traverser les autoroutes de l'information « à pieds ». Brown poursuit la description de ce nouveau paradigme de défense en montrant combien les média précèdent et impliquent aujourd'hui la conduite des conflits militaires. L'avantage est encore à la puissance capable de coordonner et de déployer en temps-réel sa puissance de feu de façon sélective, sous les regards d'une caméra. Cette perspective historique est renforcée par les analyses de Whitney-Smith qui analyse la relation entre contrôle de l'information et pouvoir depuis le cinquième siècle avant Jésus-Christ. Opposant l'ex-Union Soviétique aux États-Unis dans la période contemporaine, elle montre que le contrôle centralisé de l'information est de moins en moins synonyme de puissance. Prêchant l'abandon des ethnicités, et un contrôle local de l'information, Whitney-Smith suggère de déplacer les conflits vers les *systèmes d'interprétation*, seul véritable enjeu de cette nouvelle ère de l'information.

La seconde partie de l'ouvrage, où l'on retrouve Al Campen, Steele, Libicki, Goodden, Stein et Kuehl, est consacrée aux relations entre "cyberwar" et société civile. En imaginant une société de plus en dépendante des systèmes et des réseaux d'information, aussi bien pour sa consommation, sa santé, que pour ses systèmes financiers, cette série de contributions propose tout à la fois des mesures de sécurité électronique renforcées, et la création d'une Infrastructure Nationale d'Information (NII). Denning et MacDoran (pp.119-145) rappellent néanmoins que la vulnérabilité de cette infosphère mondiale réside dans son ancrage physique (destruction des sites d'accès, obstruction des signaux GPS, etc). Goodden propose pour sa part de dédier cette future infrastructure à la conquête et à la sécurité économique.

La troisième partie analyse concrètement le déploiement des moyens offensifs pour la conduite des conflits informationnels. Kuehl invite les décideurs américains à repenser leur géoéconomie en associant à un meilleur contrôle de l'infosphère des capacités destructrices non-léthales. Il établit une liste des cibles nationales critiques qu'il faut dès lors protéger : « systèmes de propagande nationaux », « infrastructure d'information », etc.

La quatrième partie de l'ouvrage est sans doute la plus intéressante. Elle s'interroge sur le devenir de la guerre dans ce nouveau paradigme. Première observation : la complexité de ces systèmes d'armes, et la nature furtive des agressions, rendra souvent impossible à la fois leur détection et l'évaluation des destructions. Deuxième observation : le niveau de sécurité de l'infrastructure existante est d'ores et déjà fragile. Transférer à la fois les ressources stratégiques, et les systèmes de commande, sur une unique et globale infrastructure d'information est une vulnérabilité avant d'être un atout. Troisième observation : les priorités de dépenses budgétaires ont intégré aux États-Unis cette nouvelle dimension "informationnelle" de la puissance, sans modifier les corps de doctrine, et la stratégie géoéconomique américaine. Comme le souligne les auteurs, « les États-Unis sont en train de se doter d'un armement qui demande plus qu'une exploitation de l'information fondée sur la sérendipité et le hasard ».

C'est une puissance américaine ajustant son assise sur un fauteuil qu'elle n'a pas fini de bâtir que nous propose cet ouvrage collectif. On retiendra cependant trois éléments :

– de toute évidence, une partie de la communauté militaire (incluant de nombreux "seniors" respectés) essaye de faire pression sur l'opinion pour faire adopter un projet d'infrastructure nationale d'information à un gouvernement peut-être jugé un peu trop proche des intérêts de Microsoft.

– un véritable corps de doctrine de la « guerre de l'information » est en train de naître aux États-Unis. L'ouvrage nous dévoile une équipe de professeurs, dirigeant un établissement dédié à l'*Information Warfare*, et supervisant des recherches pluridisciplinaires en coopération avec des institutions privées et publics prestigieuses.

– un effort important de recensement, tant des menaces que des possibilités d'offensives, dans le domaine des conflits informationnels a été réalisé aux États-Unis dans les cinq dernières années.

La qualité des réflexions conduites dans cet ouvrage ne peut nous amener qu'à nous interroger sur la pauvreté des efforts européens en la matière.