



## Entretien avec Marc Hecker, chercheur au Centre des études de sécurité de l'IFRI, co-auteur de *War 2.0. Irregular Warfare in the Information Age*

**La thématique de l'impact des médias comme des systèmes de communication modernes sur la guerre – mais aussi, par ricochets, sur la conduite de la politique – n'est pas neuve, comme vous le rappelez dans votre ouvrage. Aussi, quel est le facteur déclencheur du passage de la guerre « 1.0 » à la guerre « 2.0 » ?**

Depuis une quinzaine d'années, l'environnement médiatique, d'une part, et la guerre, d'autre part, ont connu de profonds bouleversements. Du côté des médias, l'émergence d'Internet et, surtout, du web 2.0 constituent une véritable révolution. Si les médias traditionnels conservent pour le moment la haute main sur la définition de l'agenda médiatique et, dans une certaine mesure, politique, ils utilisent néanmoins de plus en plus de sources provenant du web. Aujourd'hui, le monopole des journalistes professionnels sur la production de l'information est mis à mal. Chaque citoyen peut désormais transmettre des informations et partager des analyses en ouvrant un blog ou en participant à des « communautés de pratique » virtuelles conçues

comme de véritables plates-formes d'échange. Les militaires créent aussi des blogs – appelés « milblogs » – et forment également des « communautés de pratique » virtuelles comme le Army Rumour Service (ARRSE) au Royaume-Uni. Les manifestations ayant fait suite à l'annonce de la réélection de Mahmoud Ahmadinejad en Iran ont montré l'importance que peuvent avoir les « réseaux sociaux » comme Facebook ou les outils de « microblogging » comme Twitter dans la transmission d'informations. Les médias traditionnels, soumis à la censure, semblaient alors dépendants du web 2.0 et la plupart des images diffusées à la télévision avaient été filmées par les manifestants eux-mêmes, à l'aide de téléphones portables, puis diffusées sur des plates-formes de partage de vidéos comme YouTube. En somme, en l'espace de quelques années, les médias sont devenus plus interactifs, plus « collaboratifs » et plus sociaux.

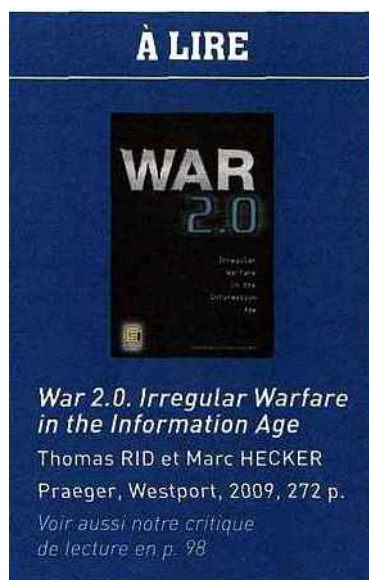
Dans le même temps, les guerres sont elles aussi devenues plus sociales. Nous sommes passés du paradigme

de la guerre classique, où deux armées régulières s'affrontent sur un champ de bataille donné, à celui de la « guerre au milieu des populations », pour reprendre l'expression employée par le général britannique Rupert Smith. Dans les guerres d'aujourd'hui, l'objectif n'est pas d'annihiler l'adversaire mais de convaincre la population locale de la légitimité de l'intervention en cours. Pour cela, il faut des actes – instauration d'un environnement sûr, construction d'écoles, d'hôpitaux, etc. – mais aussi un véritable travail d'explication qui passe par la multiplication des contacts avec la population et une importance accrue accordée à la communication. La question posée dans *War 2.0* est la suivante : que se passe-t-il quand les deux tendances qui viennent d'être décrites se rencontrent ?

Avec le co-auteur du livre, Thomas Rid, nous distinguons deux modèles. La « guerre 1.0 » et la « guerre 2.0 ». La « guerre 1.0 » est le modèle qui a culminé avec le renversement, en quelques semaines, du régime de Saddam Hussein en Irak. Elle se caractérise par l'usage massif de la force, l'utilisation d'armes de haute technologie et la volonté de détruire rapidement le ou les « centre(s) de gravité » de l'ennemi pour que la guerre soit la plus courte possible. Les technologies de l'information et de la communication sont essentiellement utilisées en interne, pour tenter d'éliminer le « brouillard de la guerre », de réduire les « frictions » et de fluidifier le processus de « command and control ». La communication externe est considérée comme secondaire et ne préoccupe pas particulièrement les combattants. La communication est confiée aux officiers de presse et la division du travail entre « communicants » et « combattants » est très nette.

Dans le modèle de la « guerre 2.0 », cette division du travail est atténuée car la distinction même entre opérations militaires et politiques devient plus floue. Le

modèle de la « guerre 1.0 » s'est heurté au défi de l'asymétrie où les progrès sont lents, la reconstruction difficile et l'obtention de l'adhésion de la population locale laborieuse. Dans la « guerre 2.0 », qui s'incarne dans les insurrections en Irak et en Afghanistan, la technologie montre ses limites. Il n'est plus question d'une victoire rapide par un usage massif de la force. Le facteur humain redevient essentiel, dans le domaine du renseignement notamment. La communication externe acquiert une importance qu'elle



n'avait pas auparavant. Il s'agit à la fois de persuader la population locale que les armées occidentales ne sont pas des armées d'occupation et de convaincre la population nationale – celle des pays occidentaux – que le déploiement de milliers de soldats est nécessaire.

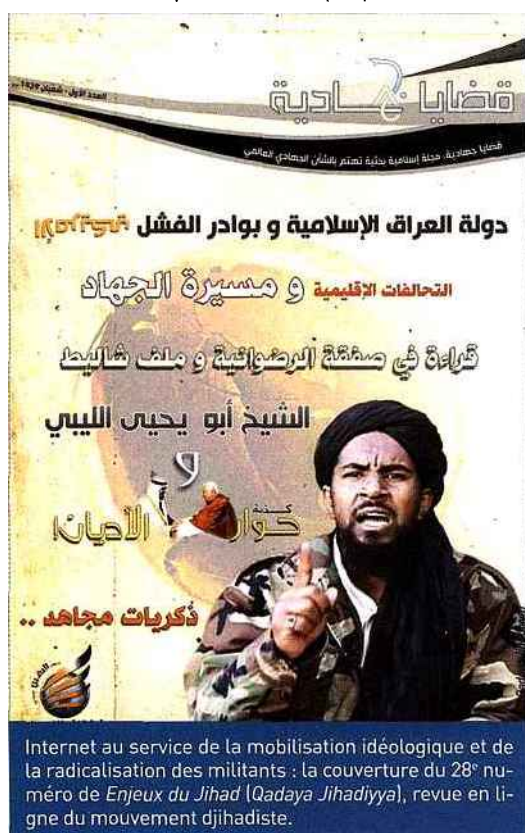
**L'explosion du nombre des connexions Internet et de téléphones mobiles est impressionnante. En quoi cela affecte-t-il la conduite des opérations insurrectionnelles pour des entités telles que les talibans ou al Qaïda ? Distinguez-vous la possibilité d'une radicalisation de la « netwar » que**

**proposaient Arquilla et Ronfeldt ? A-t-on éventuellement affaire à autre chose que la « netwar » ?**

Il convient de distinguer ici les téléphones mobiles d'Internet et les insurrections locales (les talibans) du terrorisme transnational (al Qaïda). Commençons par les téléphones portables qui, effectivement, connaissent une véritable explosion, en particulier dans les pays du Sud. Au Pakistan, le nombre d'utilisateurs de téléphones portables se situait aux alentours de 5 % en 2004. Il a dépassé les 50 % en 2008. La croissance se poursuit aujourd'hui, mais à un rythme moindre. Il se pourrait qu'en 2011, 75 % des Pakistanais possèdent un téléphone mobile. Autres chiffres étonnants : au quatrième trimestre 2007, les quatre pays qui ont connu la croissance la plus forte du nombre d'utilisateurs de téléphones mobiles étaient l'Ouzbékistan (avec une progression de 96 %), l'Iran (94,5 %), l'Afghanistan (92,9 %) et la Sierra Leone (89 %). Les effets du téléphone portable en période de guerre sont multiples et n'ont pas encore fait l'objet d'une étude détaillée. Dans *War 2.0*, plusieurs exemples sont donnés. En 2008, les talibans ont lancé un ultimatum aux compagnies locales de téléphonie mobile pour que les transmissions soient coupées pendant la nuit. Ils craignaient que leurs déplacements nocturnes ne soient relatés en temps réel par les détenteurs de téléphones portables. Cette requête n'ayant pas été satisfaite, les talibans ont fait sauter plusieurs antennes-relais. Une autre illustration est celle de la guerre de 2006 entre Israël et le Hezbollah. Au cours de cette guerre, nombre de soldats israéliens sont partis combattre avec leur téléphone et ils ne se sont pas privés de communiquer avec leur famille, leurs amis et, parfois, des journalistes. En outre, les journalistes n'ont pas manqué d'appeler les officiers sur leur mobile pour obtenir des informations. Marqués par l'ampleur des fuites, les responsables militaires israë-

liens ont décidé d'interdire aux soldats d'emporter leur téléphone lors de la guerre à Gaza de janvier 2009

Le cas d'Internet est différent. L'une des conclusions de *War 2.0* est qu'Internet favorise les groupes terroristes mais est susceptible de brider les insurrections. Pour la mouvance al Qaida, Internet a été un véritable outil de résilience sans lequel elle n'aurait pas pu se transformer



et se décentraliser comme elle l'a fait après la destruction des camps d'entraînement en Afghanistan. En se reposant trop sur Internet, al Qaida s'est toutefois coupée de son éventuelle base populaire. Certains ont parlé au sujet d'al Qaida d'« insurrection globale ». Il s'agirait plutôt d'une insurrection globale ratée. Les dirigeants d'al Qaida souhaitent soulever l'*oumma* contre les Occidentaux mais ils ont échoué. Aujourd'hui, la mouvance djihadiste internationale n'est probablement plus en mesure d'inverser la tendance. Elle est contrainte de se cantonner à des actes de terrorisme, tout en s'appuyant sur des insurrections locales. Ceci étant, Internet est un

puissant outil pour un groupe terroriste transnational. Il ne permet pas uniquement de diffuser de la propagande mais sert aussi à recruter, à trouver des financements et à échanger des conseils techniques.

En ce qui concerne le concept de « netwar », il a été créé par Arquilla et Ronfeldt en réaction à celui de « cyberwar » qu'ils jugeaient trop « techno ». Arquilla et Ronfeldt ont eu le grand mérite de comprendre, dès le milieu des années 1990, que les réseaux reposaient aussi sur des dynamiques sociales et que la solution ne pouvait pas être que technologique. Si le concept de « netwar » n'est pas utilisé dans *War 2.0*, c'est qu'il dépasse largement le cadre de la guerre pour entrer dans celui de la criminalité, voire de la délinquance. Arquilla et Ronfeldt incluent dans leur étude des catégories comme les gangs, les hooligans ou les anarchistes. *War 2.0* étudie les armées et la manière dont elles font face aux insurgés et aux groupes terroristes.

**Les armées occidentales – vous examinez plus particulièrement les cas américain, britannique et israélien dans l'ouvrage – sont-elles adaptées à cette évolution ? Leurs organisations ne sont-elles pas trop marquées par les hiérarchies ? Faut-il aller vers une augmentation de la décentralisation et un accroissement de l'initiative ?**

Les armées sont des organisations complexes marquées par une forte division du travail. Comme toute bureaucratie, elles ont besoin de hiérarchies. Il serait impossible de gérer des dizaines de milliers d'hommes sans hiérarchie et sans de multiples procédures. Une organisation pyramidale pose néanmoins un certain nombre de problèmes quand l'adversaire est organisé différemment, de manière plus horizontale et plus souple. Le principal défi est peut-être celui de la rapidité. Une organisation fortement hiérarchisée prend plus de temps à réagir car la réaction doit être validée par différents échelons avant d'être mise en œuvre. Dans le domaine de la communication, cela signifie que plusieurs heures voire plusieurs jours peuvent s'écouler avant qu'une information ne soit rendue publique. Or, à l'ère de CNN et de Twitter, chaque minute compte. Pendant la guerre de l'été 2006, l'armée israélienne a réagi plusieurs heures après l'attaque contre la corvette Hanit au large de Beyrouth, bien après le Hezbollah.

La décentralisation et l'accroissement de l'initiative peuvent effectivement permettre de gagner du temps. Les officiers de presse les plus jeunes devraient être



L'un des effets de la « reconstruction » afghane est d'augmenter la couverture GSM sur le pays, qui peut, en retour, être utilisée par les talibans pour surveiller les mouvements de l'ISAF. Mais l'ISAF peut aussi écouter : éternel jeu du chat et de la souris...

en mesure de communiquer sans que leur message ne soit *a priori* valide par leur chef. Il s'agirait d'appliquer une forme d'*Auftragstaktik* dans le domaine de la communication. La hiérarchie militaire doit comprendre que les erreurs de communication ne sont pas nécessairement lourdes de conséquence. En communiquant plus vite, les erreurs risquent d'augmenter. Mieux vaut toutefois publier une information imparfaite rapidement qu'une information parfaite trop tard, quitte à corriger certains détails ultérieurement.

Les trois armées étudiées dans *War 2.0* ont à des degrés divers intégré la nécessité de s'adapter au nouvel environnement médiatique. L'armée américaine travaille avec des blogueurs comme Michael Yon et encourage les « communautés de pratique » virtuelles à l'instar de *Companycommand* ou *Platoonleader*. L'armée israélienne a ouvert sa propre chaîne sur *Youtube* pendant la guerre à Gaza de janvier 2009, où elle a publié des dizaines de vidéos qui ont été vues par des millions d'internautes et reprises par les médias traditionnels.

Le ministère de la Défense britannique est quelque peu en retrait, mais il n'hésite pas, par exemple, à intervenir publiquement sur le *Army Rumour Service* (ARRSE). L'armée française ne fait pas partie des cas d'espèce étudiés dans *War 2.0*, mais elle accuse un certain retard dans l'utilisation des nouvelles technologies de l'information et de la communication.

**Un certain nombre de vos recommandations, notamment au niveau de la reconsidération du rôle des populations dans la guerre, sont en cours d'application – faire changer les cultures des armées est cependant complexe et long. Mais vous indiquez également qu'il ne faut pas surestimer le « facteur 2.0 ». Pensez-vous qu'à terme, les États disposeront effectivement des moyens de « percer » ces réseaux ?**

Le message de *War 2.0* est double : il ne faut pas surestimer le « facteur 2.0 », mais il ne faut pas non plus le sous-estimer. Les nouveaux outils de communication ne peuvent plus être négligés, mais il ne faut pas non plus oublier les supports de communication classiques. Les in-

surfections ancrées localement utilisent en fait davantage les outils de communication traditionnels – notamment la radio ou plus simplement encore les affiches – qu'Internet. Toutefois, les changements sont extrêmement rapides et le plus important est peut-être de créer une culture de l'observation et de l'adaptation aux innovations. Dans son *Dictionnaire des idées reçues*, Gustave Flaubert définissait l'innovation en deux mots : « toujours dangereuse ». Les innovations ne sont bien sûr pas toujours dangereuses, mais pour pouvoir les utiliser à bon escient, il faut encore comprendre leur fonctionnement et les dynamiques sociales qu'elles sont susceptibles d'engendrer.

Il ne s'agit pas de « percer » les réseaux – notamment sociaux – comme on percerait un coffre-fort. Il s'agit d'en comprendre la logique et de voir qu'ils peuvent avoir un effet bénéfique pour les armées. *Companycommand* et *Platoonleader* ont permis aux jeunes officiers d'échanger des conseils tactiques extrêmement précieux. *Facebook* pourrait être utilisé par les armées pour recruter. Dans la même logique, plutôt que de dépenser des sommes non négligeables en publicité à la télévision pour tenter d'attirer de nouvelles recrues, l'armée française pourrait diffuser des clips sur *Youtube* ou *Dailymotion*. Après tout, les jeunes que cherchent à recruter les armées passent plus de temps devant leur ordinateur que devant leur télévision.

Le phénomène 2.0 a une dynamique « *bottom up* » qui inquiète légitimement les armées habituées à fonctionner de manière « *top down* ». Ceci étant, les armées doivent dépasser le stade initial – celui du rejet voire de l'interdiction – pour aller dans le sens de la responsabilisation et de l'utilisation raisonnée.

Entretien réalisé par Joseph Henrotin  
le 28 juin 2009