Les réseaux sociaux ont un impact sur la Défense comme :

– Moyens d'expression (fonction média) : propagation et d'opinions qui deviennent « contagieuses » et conflits potentiels à propos des messages et de leur surveillance (avec l'éventuel risque de fuites ou de bavures)

– Liens (fonction organisation) : les réseaux rassemblent des communautés auxquelles ils offrent des outils de coordination, de partage d'expertise et d'action stratégique. Ils favorisent des mobilisations basées sur des objectifs décidés en commun, souvent très brusquement et comme spontanément.

– Armes (fonction de lutte) : même lorsque celle-ci porte sur des enjeux bénins (comme les mouvements de consommateurs), les réseaux sociaux sont efficaces pour mobiliser, faire passer de l'opinion à l'action, et affronter un adversaire, en ligne ou dans la rue. Accessoirement, ils sont aussi les vecteurs d'attaques informatiques destinées à dérober de l'information, à saboter des systèmes et à déstabiliser un adversaire.

Du point de vue de la Défense, leur développement pose des questions :

– de contrôle (y compris la sécurité des réseaux « internes » comme ceux qu'utilisent les soldats),

– de veille ou détection des signaux faibles et d'interprétation des mouvements collectifs à travers le contenu des échanges, éventuellement d'anticipation de futurs comportements.

– de synergie : utiliser au mieux les potentialités des réseaux en termes d'intelligence collective et de décision rapide et efficace

– et de ce qu'il faut bien appeler propagande et contre propagande.

La vision classique de la cyberdéfense et de la cybersécurité sépare l'élément technique (empêcher que des acteurs malveillants ne portent atteinte à la confidentialité, à l'intégrité ou à la disponibilité de données) et l'élément politique (la façon dont l'autorité peut empêcher la circulation de contenus interdits) ; or les réseaux sociaux rendent les deux dimensions inséparables. D'où de nouvelles règles du jeu où, par exemple, face à des attaques asymétriques s'en prenant aussi bien à des cerveaux électroniques qu'à des cerveaux humains (cyberattaques plus propagande), les « forts » ripostent parfois en imitant les techniques des « faibles », militants, protestataires..

Armées, médias et réseaux 2.0

Les forces armées sont désormais peu ou prou « sur » les réseaux sociaux : des comptes Facebook, Youtube, Twitter ou autres donnent des informations de base sur leur action ou répondent à des questions comme celles de futurs engagés. Mais cet emploi indispensable et minimaliste – un média économique auquel les jeunes sont réceptifs – ne recouvre qu'une part

des possibles.

Des armées se sont déjà engagées dans la guerre des tweets et des images : certaines lancent des défis à leurs adversaires ; elles fournissent à leurs partisans, aux neutres ou aux médias internationaux des vidéos ou « éléments de langage » qui légitiment leur action. Ainsi Tsahal versus le Hamas : une guerre de l'attention par « gazouillis » interposés dont l'enjeu était, en 140 caractères et par hyperliens, d'attirer le plus de visiteurs vers ses déclarations ou ses photos. Pour prouver les crimes de l'adversaire, si possible démonter ses mensonges, et, au moins côté Tsahal, persuader que ses opérations sont menées avec le souci maximal d'épargner des vies humaines.

Dans un autre registre, l'armée britannique a récemment présenté sa doctrine de communication stratégique : l'armée entière, jusqu'au plus humble soldat, et par tous les canaux de communication, doit décliner le « grand récit » (*narrative*) ou structure d'argumentation en de multiples sous-récits adaptés aux publics divers, toujours au service des intérêts nationaux. Dans une perspective d'influence globale, sans états d'âme et sur fond d'unanimité nationale, les médias sociaux sont fortement encouragés du « *miliblog* » aux réseaux de soutien des civils aux « *boys*« .

Dans la culture stratégique anglo-saxonne, *soft* (ou *smart*) *power*,*nation branding*, *storytelling* et e-*diplomacy* se déclinent sur les réseaux sociaux et en termes de *cyberpower*. On parle d'une stratégie d'espace-information où il serait aussi important d'agir vite et précisément que dans l'espace physique.

Les États-Unis s'expriment officiellement non seulement à travers, mais aussi à propos des réseaux sociaux : la stratégie de « *21st Century Statecraft* », le soutien sans frontière à la liberté d'Internet voire l'aide aux cyberdissidences, le développement des réseaux considérés comme intrinsèquement porteurs de valeurs universelles (et partant favorables aux intérêts américains). Les centres de recherche stratégique états-uniens, déjà familiarisés avec les notions de « *Netwar* » ou de « *network centric warfare* » sont ouverts à l'idée qu'une société économiquement, culturellement, politiquement, bouleversée par les réseaux 2.0, doit accepter un changement quant à la forme du conflit.

Certains la théorisent en termes de capacité offensive reposant sur la dominance informationnelle (tout savoir et se coordonner très vite), de convergence d'éléments dispersés (lutte « en essaims »), ou,de domination réticulaire, tandis que d'autres exaltent « l'organisation sans organisations » chère à Clay Shirky…

Les réseaux sociaux se sont montrés efficaces (mais pas à chaque fois) pour combattre un gouvernement qui contrôle les médias classiques ou pour organiser une manifestation sans l'appui d'un parti, d'une bureaucratie, de médias de masses. Ce sont des outils de mobilisation pour la population, la diaspora, l'opinion internationale. Ils sont désormais utilisables par les multitudes et pour diffuser la parole venue de la base ; ils illustrent le slogan « ne haïssez plus les médias, devenez les médias ».

Le rapport entre forts et faibles est aussi déterminé par la lutte de l'épée et du bouclier. Plus se développent des techniques de surveillance et de censure (comme le *Deep Packet Inspection*),

plus apparaissent des techniques de contournement, anonymisation, connexion « sauvage », cryptologie… Du côté de la répression comme du côté de la dissidence, la sophistication technique s'accroît et la courbe d'apprentissage des acteurs s'améliore.

Les événements de Syrie fournissent un exemple d'une guerre civile numérique qui redouble une guerre par le fer et par le feu : réseaux sociaux infiltrés ou surveillés, contre-offensives de la *Syrian ElectronicArmy*, y compris hors frontières, coupure provisoire d'Internet aux*Border Gateway Protocols (*pour couper l'Internet du pays un moment*)*…. et mobilisation de communautés adverses -pro et anti Bachar el Assad.

Les médias 2.0, supports des réseaux sociaux confèrent, à condition d'être bien employés, une chance supérieure de faire prévaloir son message dans diverses configurations : communication de l'armée ou de l'État à destination de sa propre population ou hors frontières, expression protestataire, tentative des autorités de submerger ce discours sous des messages favorables, mais aussi intervention de groupes transnationaux qui vont de l'ONG aux groupes hacktivistes comme Anonymous.

L'efficacité stratégique des réseaux tient surtout au fait que l'interaction y compte au moins autant que l'expression et qu'ils ont de multiples facettes. Ils sont notamment efficaces pour « faire l'agenda » (y compris celui des médias classiques) en décidant ce qui fait débat, bref ce à quoi il faut penser plutôt que ce qu'il faut penser. Leur faculté de mobiliser très vite des « flux d'attention » à travers le monde entier reste pour le moment inégalée.

Stratégiquement parlant, ils ne servent pas seulement de champs à une compétition « capacitaire » (faire mieux que le concurrent, atteindre davantage de monde, être plus rapide et plus performant), il s'y pratique aussi des techniques agressives indirectes et occultes. Que ce soit pour faire prédominer sa thèse sur celle de l'adversaire, une lutte de l'opinion, ou pour attaquer le système d'expression et d'information de l'adversaire, y compris par des logiciels malicieux.

Dans l'optique de la cyberdéfense, les réseaux sociaux peuvent servir de vecteurs pour des attaques destinées à voler des données, à perturber des systèmes informationnels et infrastructures stratégiques ou à exercer une action psychologique perturbante.

Mais il est aussi possible les considérer comme des outils d'alerte de risque ou des lanceurs d'alerte, comme des réserves d'information ouvertes, comme des enjeux de souveraineté, etc.

Bref, la dimension stratégique se retrouve partout.

Source : HUYGUE.FR