Avril 2012

Fiche de l'Irsem n° 16

Internet et la Défense (1) : un nouvel environnement pour la communication

Benjamin LOVELUCK
Irène EULRIET

Pour citer ce document :
Benjamin LOVELUCK,
Irène EULRIET
« Internet et la Défense (1) : un nouvel environnement pour la communication »
Fiche de l'Irsem n° 16,
avril 2012, 9 pages
http://www.irsem.defense.gouv.fr

Avril 2012

Internet et la Défense (1) : un nouvel environnement pour la communication

Internet entretient des liens intrinsèques avec les armées. Issu d'un projet du gouvernement américain de mise en réseau d'ordinateurs, son ancêtre ARPANET répondait à plusieurs objectifs. Il s'agissait tout d'abord de partager les ressources informatiques, ainsi que de parvenir à une meilleure interaction homme-machine. Dans un deuxième temps, l'adoption d'une architecture en réseau distribuée sera présentée comme un moyen d'assurer la résilience des communications et d'éviter ainsi une rupture de la chaîne de commandement. ARPANET a donc représenté un enjeu important dans le contexte de la réflexion sur le 'Commandement et contrôle' militaires pendant la guerre froide.

À partir des années 1970 cependant, ARPANET s'est graduellement affranchi du giron militaire, et son prolongement à travers Internet en tant que « réseau de réseaux » s'est progressivement mis en place. Le monde civil se l'est alors approprié.

Aujourd'hui, Internet fait partie du quotidien d'un nombre croissant d'individus. En France, la proportion de la population utilisant la toile est passée de 14,4 % à 80,1 % entre 2000 à 2010.[1] Le temps passé sur Internet est aussi en augmentation. Totalisant 32 mn/jour en moyenne en 2009, il ne déclasse pas encore la télévision (en moyenne 2 h/jour), mais pour certaines catégories, les hommes de 15-24 ans en particulier, le temps voué à la toile est supérieur à celui consacré à la télévision[2]. L'OCDE fait aussi le constat que les jeunes sont très consommateurs d'Internet : ils ont « presque deux fois plus de contacts avec l'Internet et les autres supports que l'ensemble des utilisateurs »[3].

[1] Selon les données colligées par l'Union internationale des télécommunications, un organisme onusien : http://www.itu.int/ITU-D/ict/statistics/, rubrique : Key 2000-2010 Country Data, onglet : Percentage of Individuals Using the Internet [consulté le 23 mars 2012]

[2] Il aurait doublé, selon l'INSEE, entre 1999 et 2009, passant de 16mn en moyenne à 32 mn. Cf. http://www.insee.fr/fr/themes/document.asp?ref_id=ip1377#inter4 [consulté le 23 mars 2012]

[3] Groupe de travail sur l'économie de l'information, *Accès au haut débit et aux TIC et utilisation par les ménages et les individus*, DSTI/ICCP/IE(2007)4/FINAL, Paris : OCDE, 2008, p. 29, téléchargeable à : http://www.oecd.org/dataoecd/61/41/40026067.pdf

Avril 2012

Internet s'avère aujourd'hui façonné par des valeurs d'égalité, d'expression individuelle, de transparence, de libre circulation de l'information et de mise à distance de l'autorité semblant, de prime abord, antithétiques au monde militaire – celui-ci étant davantage caractérisé par la centralisation, la hiérarchisation et la confidentialité. Bien que s'accordant dès lors avec la transition culturelle effectuée dans les années 1970 par les démocraties libérales, Internet en remet également l'un des fondements en cause : la distinction public/privé. L'un des aspects les plus inédits d'Internet tient en effet à la dissolution de la séparation nette entre les domaines de la communication officielle, à caractère politique, et de la conversation privée.

Dans ce contexte, il est opportun de s'interroger sur les conséquences de ce nouvel environnement communicationnel, et de l'interpénétration des sphères publique et privée, pour la Défense et ses politiques. La question de l'impact sur le monde militaire de la massification de l'usage d'Internet à des fins de communication, à laquelle la récente étude réalisée par l'Ifri pour l'Irsem[4] propose certains éléments de réponse, fait l'objet de la présente note. Sont ici abordées les conséquences de ces nouveaux usages sur : (1) la sécurité des opérations ; (2) le contrôle de l'image de l'institution militaire ou/et des informations y afférant ; (3) les besoins internes des armées, notamment de recrutement et de formation.

Arthur L Norberg et Judy E O'Neill, *Transforming Computer Technology. Information Processing for the Pentagon, 1962-1986,* Baltimore, MD, Johns Hopkins University Press, 1996

Cardon, Dominique, *La Démocratie Internet. Promesses et limites,* Paris, Seuil, 2010

Janet Abbate, *Inventing the Internet,* Cambridge, MA, MIT Press, 1999

Fred Turner, *From Counterculture to Cyberculture. Stewart Brand, the Whole Earth Network, and the Rise of Digital Utopianism,* Chicago, IL and London, University of Chicago Press, 2006

1. L'usage privé d'Internet par les militaires pose-t-il des enjeux de sécurité spécifiques pour les opérations ?

Les communications personnelles des soldats, en devenant plus nombreuses et plus détaillées grâce à l'appareillage dont ils disposent (ordinateurs, téléphones, appareils photos numériques) et, en étant parfois consignées sur le web sur des plateformes non sécurisées (Facebook, Twitter, YouTube, blogs,

[4] Marc Hecker et Thomas Rid, *Utilisation et investissement de la sphère Internet par les militaires*, Paris : IRSEM, 2012

forums, etc.), sont susceptibles de se trouver exposées : soit que l'information mise en ligne par un soldat se retrouve diffusée hors d'un réseau restreint par inadvertance (par le soldat en question ou par ses proches); soit que les communications aient été interceptées par l'ennemi disposant de compétences plus ou moins poussées en *hacking*. La question des enjeux de sécurité spécifiques induits par l'usage d'Internet par les militaires à des fins personnelles est dès lors posée.

C'est dans ce cadre que l'Irsem a commandé une étude visant, entre autres, à évaluer les risques issus de cet usage. L'une des principales conclusions de l'enquête confiée à l'Ifri est qu'une majorité écrasante d'usagers militaires comprend les risques qu'ils peuvent encourir, ou faire encourir, en divulguant des informations sur leurs activités par le biais d'Internet. Utilisant les réseaux sociaux principalement pour communiquer avec leurs proches, ils en saisissent la portée et font preuve, dans la pratique, de prudence. L'usage qu'ils font d'Internet est ainsi en phase avec la vision du commandement militaire français, pour qui domine l'idée que les militaires s'auto-disciplinent dans la mesure où ils respectent leurs engagements vis-à-vis du secret militaire et du devoir de réserve.

Malgré la bonne volonté des individus, il paraît inévitable que des informations circulant sur Internet puissent compromettre une mission. L'étude signale en effet que des détails stratégiques peuvent être transmis à l'insu des utilisateurs : un cas typique est celui des photos, qui fournissent en elles-mêmes beaucoup d'informations, et dont les métadonnées peuvent par exemple contenir un positionnement GPS (géo-localisation) lorsqu'elles sont prises avec un téléphone intelligent (*smartphone*). L'étude révèle également que des conclusions importantes peuvent être déduites d'informations *a priori* banales : en ceci, l'analogie qu'avait pu établir le commandant Ray Ceralde en 2007 entre la diffusion de données anodines sur Internet et l'accroissement subit du nombre de commandes de pizzas par le Pentagone ne manque pas de pertinence.[5] L'une et l'autre peuvent, selon les circonstances, livrer de précieuses indications sur la nature d'une opération ou son imminence.

L'expérience des Etats-Unis et du Royaume-Uni démontre cependant la difficulté (en termes d'acceptation sociale et de capacité technique) de mettre en œuvre une politique basée sur l'interdiction. Les approches privilégiant la pédagogie et la sensibilisation aux dangers paraissent plus porteuses. Ceci comprend une sensibilisation aux fonctionnalités (et aux paramétrages par défaut) des outils de l'Internet et n'exclut pas d'emblée la mise en place de dispositifs de contrôle : les Etats-Unis ont en effet déployé une unité spéciale chargée de surveiller les activités des militaires sur Internet[6]. En France,

[5] Comme noté dans l'étude. Cf. Hecket et Rid, *op. cit.*, p. 81.

[6] « Aux Etats-Unis, une *Joint Web Risk Assessment Cell* (JWRAC) existe depuis 1999. (…) L'*Army* dispose aussi d'une telle unité – appelée *Army Web Risk Assessment Cell* (AWRAC). La taille précise et les méthodes employées par l'AWRAC n'ont pas été rendues publiques. On sait en revanche qu'elle est composée à la fois de militaires d'active et de réservistes, et qu'elle est aidée dans sa tâche par des sous-traitants. Elle surveille non seulement les sites officiels mais aussi les blogs, notamment ceux que tiennent les soldats déployés en Irak et en Afghanistan. » (Hecker et Rid, *op. cit.*, p. 96-97)

l'approche privilégiée repose principalement sur la « sensibilisation »[7] ou la « responsabilisation », plutôt que sur l'interdiction et la surveillance – avec toutefois des consignes claires dans certains cas[8].

L'usage que font les militaires d'Internet à des fins personnelles est donc responsable, pour une immense part. Cependant, il ne peut pas échapper à des détournements ou des effets non-voulus, et ce, malgré les mesures qui pourront être prises. De tels détournements ou effets non-voulus pourraient s'avérer dévastateurs dans le cadre d'opérations. Mais si les opérations constituent des situations particulièrement sensibles pour la Défense, les enjeux de communication qu'elles concrétisent se trouvent à vrai dire à la croisée de problématiques plus générales concernant la gestion et le contrôle des flux de communication à l'ère de la libre circulation de l'information.

Arquilla, John et Douglas A Borer (dir.), *Information Strategy and Warfare. A Guide to Theory and Practice*, London and New York, Routledge, 2007

Roberts, Alasdair S, *Blacked Out. Government Secrecy in the Information Age*, Cambridge and New York, Cambridge University Press, 2006

Sifry, Micah, *WikiLeaks and the Age of Transparency,* New York, OR Books, 2011

2. Quelle approche adopter afin de gérer et de contrôler l'image de l'institution militaire et la diffusion d'informations s'y rapportant ?

Les technologies de l'information et de la communication multiplient les sources potentielles de contenus – chaque utilisateur pouvant en générer – ainsi que les supports de diffusion. Les possibilités de propagation de représentations ou d'informations affectant (de manière positive ou négative) l'image de l'institution militaire par des individus affiliés ou non au ministère de la Défense, via des *tweets*, des blogs, des réseaux sociaux, des plateformes ou des forums, et ce, quel que soit le format (écrit, vidéo ou audio) sont, en théorie, augmentées. Elles présentent donc de nouvelles contraintes (mais aussi de nouvelles opportunités) pour le ministère de la Défense.

L'étude souligne que l'usage que font les militaires de la liberté d'expression et de partage d'information est positive dans la mesure où ceux-ci témoignent le plus souvent d'une grande loyauté par rapport à l'institution militaire. En ce qui concerne les pages les plus aisément accessibles et les plus fréquentées (par exemple certains sites institutionnels offrant la possibilité de dialoguer, tels celui du *Chairman of the*

[7] Cf. la directive du général Elrick Irastorza en 2008 (n° 215/DEF/EMAT/PS/BPES/DR), cité in Hecker et Rid, *op. cit.*, pp. 86-87.
[8] Cf. le guide « Communiquer en opération » de l'armée de Terre, cité in Hecker et Rid, *op. cit.*, p. 90.

Joint Chiefs of Staff (CJCS) aux Etats-Unis), les divers intervenants, en particulier les usagers militaires ou les « fanas-milis », affichent également un grand respect envers l'institution et ceux qu'ils considèrent leurs camarades. Ils tendent à s'exprimer favorablement sur l'institution. En outre, ils se mobilisent dans le cas où un commentaire jugé injuste ou inapproprié est mis en ligne (auto-régulation).

Mais il demeure que des informations considérées devoir rester internes – qu'elles soient peu flatteuses, défavorables ou contraires aux intérêts de la Défense – peuvent volontairement être rendues publiques[9]. La probabilité que ces témoignages de l'intérieur soient repris par les « grands médias » est forte, qui plus est, sitôt qu'un seuil critique est atteint sur Internet. Sans s'interroger sur leur valeur morale ou politique, divers cas problématiques pour l'institution militaire peuvent être cités ici, sur un spectre allant du bénin au grave : dans le contexte français, les images diffusées dans le cadre du film *C'est pas le pied la guerre*; dans le contexte américain, les informations révélées par WikiLeaks – qui donnent bien la mesure des conséquences que peuvent entraîner les « fuites » dans le contexte d'Internet.

Une des principales stratégies afin d'augmenter la maîtrise des contenus est d'essayer d'être présent à la source des mécanismes de diffusion et de viralité, c'est-à-dire de fournir des images directement consultables sur le web, et qui pourront être facilement partagées sur les blogs et les médias sociaux, en plus d'être disponibles pour la télévision. C'est dans ce contexte que doivent être appréhendées les initiatives des armées israélienne et allemande, rapportées dans le rapport Ifri, consistant à créer une chaîne de télévision dédiée sur YouTube. Leur portée est d'autant plus significative que le visionnage de vidéos (y compris les programmes télévisuels) par le biais d'Internet est en forte augmentation[10] et que celui-ci intervient, de plus en plus, sur des téléphones portables[11].

Les expériences allemande et israélienne sont également intéressantes dans la mesure où elles illustrent deux approches foncièrement différentes (liées au profil militaire de chacun des pays) dans la recherche de maîtrise de la diffusion des contenus issue de la « convergence » des médias : à travers sa présence sur *YouTube*, l'armée israélienne exploite pleinement les possibilités qu'offrent les nouvelles technologies en matière de tournage, de réalisation (technologie embarquée) et de rapidité de diffusion dans une perspective de communication stratégique et politique. L'armée allemande a déployé, quant à elle, une conception plus traditionnelle de la production télévisuelle à travers *Bundeswehr TV*, en créant des studios bien dotés en personnel et en moyens, dont l'activité est plus orientée vers le recrutement et la communication institutionnelle classique.

[9] Quoique le procédé ne soit pas nouveau, mais Internet en décuple les effets. Par ailleurs, il faut noter que la 'critique' fait partie intégrante de la vie de l'institution : elle permet de la faire évoluer, d'en améliorer le fonctionnement et d'en redéfinir les objectifs. La 'critique' est à vrai dire au fondement de l'ordre démocratique.
[10] Groupe de travail sur l'économie de l'information, *op. cit.*, p. 31
[11] Groupe de travail sur l'économie de l'information, *op. cit.*, p. 19

Avril 2012

Le nouvel environnement de communication qu'est Internet comprend dès lors un certain nombre de contraintes pour l'institution militaire. Trois peuvent être mentionnées ici. Premièrement, des ressources supplémentaires doivent être allouées en vue de produire, de gérer et de contrôler les contenus. Vient, deuxièmement, l'obligation de prendre en compte les « intermédiaires Internet » : alors que les institutions militaires conservent un ancrage national déterminant, ce sont ces interfaces non-étatiques[12], opérant la plupart du temps à l'échelle planétaire, qui offrent à des utilisateurs potentiellement mondialisés (lecteurs, auditeurs, spectateurs, producteurs de contenus) l'infrastructure indispensable à l'échange d'informations. La troisième contrainte tient à la nécessaire extension des pratiques établies entre institution militaire et journalistes spécialisés. Si Internet permet de contourner les médias dits traditionnels, l'organisation de la coproduction d'informations avec un nombre d'utilisateurs bien plus large, et dont le profil est bien moins homogène que la catégorie socioprofessionnelle des journalistes, présente néanmoins des incertitudes[13].

Jenkins, Henry, *Convergence Culture. Where Old and New Media Collide*, New York, New York University Press, 2006

Sheldrake, Philip, *The Business of Influence. Reframing Marketing and PR for the Digital Age*, Chichester, West Sussex, Wiley, 2011

Solove, Daniel J, *The Future of Reputation. Gossip, Rumor, and Privacy on the Internet*, New Haven, CT and London, Yale University Press, 2007

Wasik, Bill, *And Then There's This: How Stories Live and Die in Viral Culture*, New York, Viking, 2009

3. **Comment, et jusqu'où, Internet peut-il être utilisé en vue du recrutement et de la formation ?**

La Défense peut bénéficier grandement des évolutions liées à l'usage d'Internet en tant que recruteur et employeur. Les potentialités que recèlent Internet et ses supports pour satisfaire les besoins de l'institution sont d'ailleurs déjà exploitées[14]. Ils permettent d'atteindre les catégories d'âge recherchées et facilitent un meilleur ciblage des viviers au moyen du marketing web et de l'analyse décisionnelle. Ceci est d'autant plus vrai dans un contexte où la fracture numérique, c'est-à-dire l'inégal accès aux moyens matériels permettant d'utiliser Internet, tend à se résorber, notamment grâce aux téléphones portables

[12] Les intermédiaires sont majoritairement américains, cependant.
[13] Cf. Hecker et Rid, *op. cit.*, pp. 33-35
[14] Cf. Hecket et Rid, *op. cit.*, p.47-55.

intelligents[15]. Internet, couplé à l'usage du téléphone portable, élargit dès lors considérablement le rayonnement de l'effort de recrutement.

Les nouvelles technologies de l'information offrent également la possibilité de dispenser des formations moins onéreuses et susceptibles d'être suivies à distance, entre autres par le biais de *serious games*. Cette possibilité, pour intéressante qu'elle soit au niveau pédagogique et économique, pose directement la question de la socialisation des militaires. Ici, les différentes pratiques sociales que favorise Internet doivent être prises en compte. Elles correspondent tout d'abord à un approfondissement des aspects performatifs de l'individualisme contemporain : les manières de se présenter et de construire activement son identité et ses relations sociales sur Internet peuvent être comprises comme des « techniques relationnelles ». Ensuite, les activités en réseau, notamment les jeux, constituent un espace d'apprentissage de la règle, de la hiérarchie, de l'autorité, et un lieu d'expérimentation de différents rôles sociaux (à travers les avatars). Procurant une représentation, et parfois même une expérience, du collectif, les activités en réseau recèlent dès lors un potentiel socialisant souvent occulté, mais sans doute positif s'il est combiné adroitement à un enseignement classique.

Alors que les dimensions plus spécifiquement cognitives de la formation à distance constituent une question à part entière, il importe de s'interroger sur le degré de virtualité qu'il est possible d'intégrer à la formation militaire. L'enjeu principal revient ici à pratiquer une telle introduction sans compromettre les modes de socialisation générateurs du sentiment d'appartenance (esprit de corps) au fondement de l'efficacité opérationnelle. Dans ce contexte, il convient de garder à l'esprit deux choses : d'une part, l'univers professionnel militaire engage la personne, du moins en ce qui concerne les fonctions opérationnelles, bien au-delà de ce que la plupart des emplois *IRL*[16] exigent ; d'autre part, l'institution militaire elle-même recourt à des systèmes complexes dans la conduite des opérations qui modifient la relation du soldat au terrain, à l'ennemi et à la mort (relation homme-machine).

S'il est certain qu'Internet et ses outils rebattent les cartes de la socialisation, les conséquences de ces nouveaux modes relationnels ne sont, à ce jour, pas pleinement manifestes. Cependant, les armées peuvent d'ores et déjà anticiper l'avènement d'un type nouveau d'individu, dont il est possible de souligner deux caractéristiques principales : d'un côté, celui-ci manifeste le plus souvent un désir de singularisation prononcé ; de l'autre, il est également plus dépendant de réseaux relationnels rendus « persistants » par les nouvelles technologies de communication. Cette évolution, dont la Défense a été un protagoniste majeur, lui impose en retour de *tester* jusqu'où Internet et ses outils peuvent être employés dans un objectif de formation.

[15] Groupe de travail sur l'économie de l'information, *op. cit.*, p. 37
[16] *In Real Life* – « dans la vraie vie » – pour reprendre le vocabulaire des communautés de joueurs.

Beau, Frank (dir.), *Culture d'univers. Jeux en réseau, mondes virtuels, le nouvel âge de la société numérique*, Limoges, FYP Editions, 2007

Cardon, Dominique, « L'identité comme stratégie relationnelle », *Hermès*, n° 53 (2009), p. 61-66

Licoppe, Christian, *L'Evolution des cultures numériques. De la mutation du lien social à l'organisation du travail*, Limoges, FYP Editions, 2009

Taylor, T.L., *Play Between Worlds. Exploring Online Game Culture*, Cambridge, MA, MIT Press, 2006

Conclusion

A l'aune des éléments rassemblés dans cette note, il apparaît que les usages sociaux d'Internet et leurs effets peuvent faire l'objet d'analyses selon plusieurs axes : usage personnel versus usage officiel ; diffusion intentionnelle d'informations versus diffusion fortuite ; moyen de communication opérationnelle et institutionnelle ; etc. Les angles d'observation des usages individuels d'Internet, de sa (ré-)appropriation par l'institution militaire, de leurs effets croisés, voulus et non-voulus, sont aussi nombreux que les modifications qu'ils matérialisent et les innovations qu'ils appellent.

S'il fallait relever un élément fondamental, pour la Défense, au sein de ce nouvel environnement communicationnel, sans doute serait-ce le suivant : le fait que des informations soient inévitablement amenées à s'échapper et à se diffuser dans l'environnement éminemment « liquide » que représente Internet. Il s'agit d'une réalité qui est directement liée à la plus grande porosité des sphères publique et privée. La remise en cause de cette distinction atteste en effet de nouvelles pratiques sociales, de la part des individus et des institutions, engageant une reconfiguration des espaces politiques, sociaux et privés. Un nouveau vocabulaire socio-politique reste à élaborer afin d'en saisir, et d'en décrire, la spécificité.

Benkler, Yochai, *The Wealth of Networks. How Social Production Transforms Markets and Freedom,* New Haven, CT, Yale University Press, 2006 (traduction française : Benkler, Yochai, *La Richesse des réseaux. Marchés et libertés à l'heure du partage social,* Lyon, Presses universitaires de Lyon, 2009)

Beuscart, Jean-Samuel, Eric Dagiral et Sylvain Parasie, « Sociologie des activités en ligne (introduction) », *Terrains & travaux*, n° 15 (2009), p. 3-28

Denouël, Julie et Fabien Granjon (dir.), *Communiquer à l'ère numérique. Regards croisés sur la sociologie des usages,* Paris, Transvalor/Presses des Mines, 2011