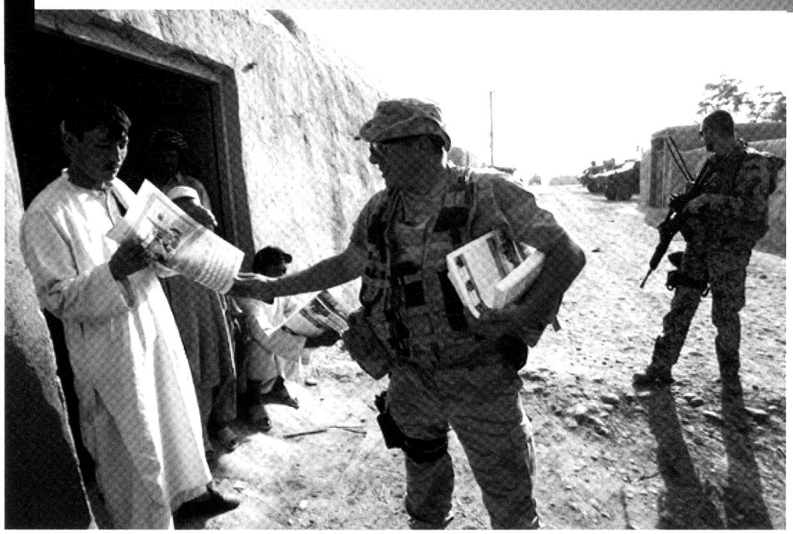
Zeitschrift: Revue Militaire Suisse
Band: - (2010)
Heft: 3

Artikel: Les opérations d'information (InfoOps) au profit de la conduite d'opérations militaires, mais aussi au profit de la politique nationale
Autor: Arcioni, Sandro
DOI: https://doi.org/10.5169/seals-514430



Diffusion d'informations en Irak, par des équipes de relations civiles-militaires (CIMIC). Photos © US Army.

Sécurité

Les opérations d'information (InfoOps) au profit de la conduite d'opérations militaires, mais aussi au profit de la politique nationale

Lt col EMG Sandro Arcioni

Dr ès Sc., chef d'entreprise

La Suisse doit pouvoir s'offrir une image digne de ce nom, mais pas comme elle l'a démontré ces derniers temps sur la scène internationale : manque de cohésion inter-départements et, surtout, manque de vision stratégique à long terme. Les InfoOps, c'est-à-dire les opérations d'information, peuvent combler ces lacunes et chapeauter la communication afin de contrôler sa cohésion et tenir compte des aspects stratégiques. C'est ce que l'on nomme, dans le monde de l'entreprise « l'intelligence économique ». Les InfoOps déterminent le moment, la manière et le destinataire, tandis que la communication est un des moyens de transmission de l'information.

De tout temps, dans la Grèce antique ou sous Napoléon, des opérations d'information ou d'influence ont été conduites pour tromper l'adversaire et préserver la liberté de manœuvre de sa propre armée. Que cela se soit vu sous la forme du Cheval de Troie ou, durant la Seconde Guerre mondiale, par des informations erronées émises par les Japonais avant l'attaque de Pearl Harbor, les opérations d'informations ont toujours eu une part d'importance dans la conduite des opérations.

Aujourd'hui, par l'importance des moyens de communication, la rapidité de cette communication, l'imbrication complète du champ d'action militaire sur le champ d'action civil et économique ou vice-versa, ce type d'opérations peut donner de part et d'autre des belligérants un avantage décisif sur la finalité de la manœuvre globale. Pour aller plus loin, si ces opérations sont bien menées, elles peuvent donner cet avantage décisif en épargnant de nombreuses vies humaines. Ce type d'opération est en général peu coûteux et tient compte de l'espace économique et civil de l'ensemble du terrain opératif. Par exemple, en France, le terme d'opérations militaires d'influence (OMI) a été remplacé par le terme d' « opérations environnementales ».

Qu'entend-on par opérations d'information ?

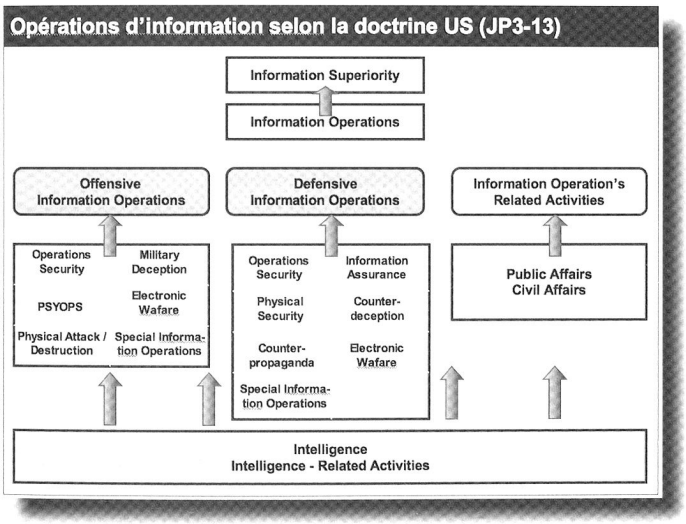
Avant de donner une définition des opérations d'information, nous décrirons ce que signifie la notion de manœuvre globale. La manœuvre globale est le processus itératif visant l'atteinte de l'effet final recherché et permettant au chef de déterminer, d'obtenir puis d'évaluer un effet sur l'adversaire et sur l'environnement par la mise en œuvre de capacités militaires ou non militaires à tous les niveaux de force engagés. Ce processus implique l'ensemble des cellules d'un état-major ou d'un poste de commandement (PC) d'une grande unité et vise à atteindre directement ou indirectement, par des effets physiques ou psychiques les centres de gravité ou les points de vulnérabilité de l'adversaire.
Même si aujourd'hui, l'OTAN a abandonné le concept de la manœuvre par les effets (EBAO : Effect Based Approach to Operations), ce sont bien des effets que nous entendons produire sur l'adversaire de façon progressive, en touchant ses points de vulnérabilité et ses centres de gravité, tout en gardant à l'esprit la finalité de la globalité de la manœuvre.
Si nous prenons maintenant la définition de l'OTAN des opérations d'information, ces opérations (IO) concernent l'emploi intégral des moyens militaires, des appuis ainsi que toutes les actions et les opérations visant à influencer, perturber, corrompre, usurper, voire neutraliser les décisions adverses humaines, comme automatisées (guerre électronique), servant à protéger les nôtres.
Ces dernières sont menées au niveau stratégique, opératif et tactique et sont définies comme étant des actions exécutées pour induire délibérément en erreur les décideurs adverses, comme parfois les décideurs alliés, par des moyens, des intentions et des opérations qui provoqueront chez l'adversaire la prise de mesures (ou d'inactions) spécifiques, qui contribueront à l'accomplissement de notre mission.

En Suisse, la définition est plus limitée et se définit comme l'ensemble des actions planifiées et conduites, appuyées

par les activités du renseignement notamment (cf. concept « HEAT ») et ayant pour but de perturber, influencer ou détruire le processus décisionnel d'un adversaire tout en améliorant et en protégeant son propre processus contre les effets de telles actions ainsi que contre tout événement involontaire ou fortuit.

Comment s'organise la conduite des opérations d'information ?

La doctrine de l'armée américaine prévoit, en matière de conduite des opérations d'information, trois parties : les opérations d'information offensives, les opérations d'information défensives et les opérations d'information relatives aux activités (c'est-à-dire transparentes).



C'est bien à une cellule InfoOps de gérer et coordonner l'ensemble des ces opérations, afin d'en garantir la concordance et l'alignement sur la finalité de la manœuvre globale. Le chef de cette cellule dépendra directement du commandant assurant la responsabilité de la manœuvre globale. L'ensemble des cellules opérant dans le domaine de l'information travailleront étroitement avec le renseignement militaire.

Pour la conduite des opérations d'information offensives, les moyens à disposition sont :

- Les opérations de sécurité « OPSEC ». Processus d'identification de l'information critique et d'analyse des mesures particulières concernant les opérations militaires et autres activités visant à identifier les actions qui peuvent être observées par les systèmes de renseignement adversaire. Détermination des indicateurs que les systèmes de renseignement adverses pourraient obtenir et qui pourraient être interprétés comme des informations critiques utiles à l'adversaire. ;
- Les opérations militaires de déception. Mesures visant à tromper l'ennemi par la manipulation, distorsion ou la falsification de preuves pour l'amener à réagir d'une manière préjudiciable à ses intérêts ;
- La guerre électronique. Toutes actions militaires impliquant l'utilisation d'électromagnétique et la mise en scène d'énergie pour contrôler le spectre électromagnétique de l'ennemi.
- « Electronique de protection ». Cette opération implique des moyens actifs et passifs mis en œuvre pour protéger le personnel, les installations et l'équipement de tout effet ennemi de la guerre électronique ennemie, qui en se dégradant, pourrait neutraliser ou détruire la capacité de combat.
- « Soutien à la guerre électronique ». Cette opération porte sur des actions visant à rechercher, à intercepter, à identifier et à localiser des sources d'énergie électromagnétique rayonnant intentionnellement ou non pour les fins de reconnaissance, de menace immédiate, de ciblage, de planification ou de conduite des opérations futures.
- Les attaques de destruction physique (létales ou cinétiques).
- Les opérations psychologiques et les opérations spéciales d'information. Ce sont des opérations planifiées pour transmettre des informations à des gouvernements, des organisations, des groupes et des individus étrangers capables d'influencer leurs émotions, leurs motivations, leur raisonnement objectif et, finalement, leur comportement.
- Les opérations spéciales d'information : sont des opérations qui pourraient faire appel au niveau politique par exemple, aux forces d'actions spéciales ou à tout autre élément extérieur.

La conduite des opérations d'information défensives met à contribution :

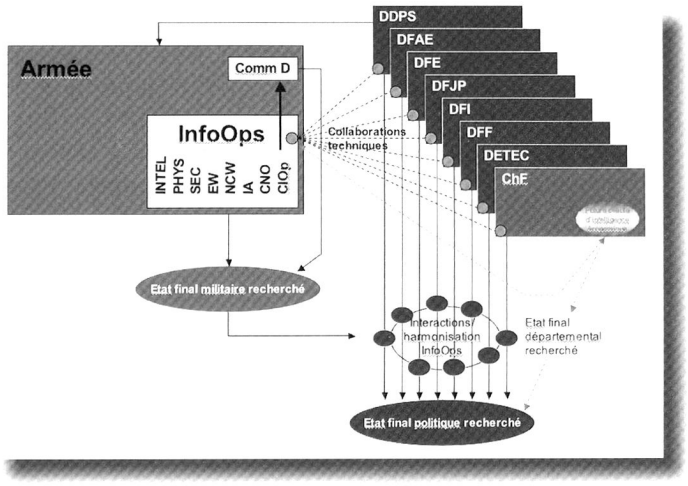
- Les opérations de sécurité (OPSEC).
- Les opérations de sûreté de l'information. Mesures qui protègent et défendent l'information et les systèmes d'information en garantissant leur disponibilité, l'intégrité de leurs données, l'authentification des utilisateurs, la confidentialité et la non répudiation. Elle tient compte aussi des capacités de réaction et de la possibilité de restauration des systèmes d'information).
- La sécurité physique. Mesures physiques visant à préserver le personnel ; empêcher tout accès non autorisé aux équipements, installations, matériel et documents, et à les protéger contre l'espionnage, le sabotage, les dommages et le vol.
- La guerre électronique, les mesures visant à protéger les systèmes d'information (disponibilité de l'ensemble des systèmes d'information, etc).
- La « *counterdeception* », c'est-à-dire les efforts visant à nier, neutraliser, diminuer les effets d'une opération de tromperie de l'adversaire.
- Le « *counterpropaganda* ».
- Les opérations spéciales d'information : sont des opérations qui se feraient de manière non létale par exemple sur des acteurs économiques et financiers adverses.

La conduite des opérations d'information relatives aux activités, c'est-à-dire par rapport à l'environnement civil : Il s'agira bien ici de l'information relayée par des spécialistes des médias, ayant pour cible une population ou un gouvernement, mais au travers des médias (télévisions, radios, presse écrite, internet). Ces opérations se font en général de manière transparente, mais coordonnées avec les opérations d'information pour éviter de prendre à contre-pied un effet désiré dans le concept de la manœuvre globale. Ces opérations sont conduites par des « Public Affairs Officers » (PAO) par l'intermédiaire des

Press Information Officers (PIO). De même, ces officiers s'occuperont de l'information de la « base arrière », c'est-à-dire d'informer les familles des militaires engagés de la situation sur le terrain, ainsi que les différents organes médiatiques du pays.

Actuellement, l'armée suisse travaille encore sur la base du Press Information Officers (PIO), qui est plus un porte-parole du commandant de la Grande Unité et un coordinateur de l'information se trouvant sur le site Internet ainsi que la rédaction des journaux de troupe. Ceci est encore très éloigné de la vision des « Public Affairs » ! Une petite entité, qui se trouve à l'Etat-major de conduite de l'Armée (J3 EM cond A, Astt 234 et 235), sous le nom d'InfoOps, se cherche actuellement une légitimité. Il est à noter que malheureusement, ni DDPS ni la conduite politique n'ont encore reconnu cette « arme » que sont les opérations d'information comme un élément stratégique. Or il s'agit là d'une clé majeure pour éviter la guerre et les pertes humaines.

La conduite en matière d'InfoOps n'est pas chose facile, car elle implique une coordination autant militaire que politique, par rapport à une vision globale. Pour comprendre les imbrications, il faut ce reporter au schéma ci-dessous représentant les liens entre les différents départements fédéraux et l'armée, indiquant les interactions possibles en fonction des actions à mener entre l'Armée (DDPS) et les autres départements en matière d'opérations d'information et d'influence.



Comment devrait s'organiser la conduite des opérations d'information à l'échelon politique en Suisse ?

Afin d'éviter des erreurs interdépartementales telles que nous venons de les vivre avec les listes de données bancaires volées en Suisse et achetées par l'Allemagne, l'affaire libyenne, l'arrêt de Roman Polanski, les diverses prises de position sur l'engagement de notre armée (par exemple au sujet de l'opération ATALANTA), sans pour autant réorganiser les différents départements, les moyens existants au sein de notre armée, sont déjà en mesure d'entraîner ou de tester ces derniers ; ils peuvent également agir à la manière d'un « ciment » interdépartemental.

Les InfoOps n'agissent pas de leur propre gré, mais sous une conduite politique. La question est de savoir à quel département revient le « *lead* ? Peut-être serait-il alors plus judicieux de confier ces activités à la Chancellerie fédérale où une cellule dédiée aux InfoOps (dénommée cellule d'intelligence économique) travaillerait étroitement avec le responsable de la communication du Conseil fédéral.
Il en va aujourd'hui de la crédibilité de notre pays. France, Allemagne, Angleterre ou Etats-Unis ont déjà franchit ce pas.

S.A

Bibliographie

US Army 3-13.4 Joint Publication (Fomerly, JP-3-58), *Miltary Deception*, 13 July 2006.

US Army DOD Directive 3600.1, *Information Operations (IO)*, SD-106 Formal Coordination Draft.

US Army CJCSI 3210.01A, *Joint Information Operations Policy* (U), 6 November 1998.

US Army CJCSI 3210.03B, *Joint Electronic Warfare Policy* (U), 31 July 2002.

US Army. JP 1, *Joint Warfare of the Armed Forces of the United States.*

US Army JP 3-0, *Joint Operations.*

US Army JP 3-05, *Doctrine for Joint Special Operations.*

US Army JP 3-08, *Interagency, Intergovernmental Organization, and Nongovernmental Organization Coordination During Joint Operations, Volume I and II.*

US Army JP 3-13, *Information Operations.*

US Army JP 3-16, *Multinational Operations.*

US Army JP 3-51, *Joint Doctrine for Electronic Warfare.*

US Army JP 3-53, *Doctrine for Joint Psychological Operations.*

US Army JP 3-57.1, *Joint Doctrine for Civil Affairs*

US Army JP 3-61, *Public Affairs.*

Armée Française, PIA – 03.152, *Concept interarmées des opérations d'information*, 11 mars 2005

Armée Française, PIA – 03.252.1, *Doctrine interarmées de la communication opérationnelle*, 26 juillet 2007

Armée Française, PIA – 03.252, Doctrine interarmées des opérations d'information, 29 mai 2006

Armée Française, PIA – 03.253, Doctrine interarmées des opérations d'influence, 5 mars 2008

Colonel Chauvancy, F., (2008), Influencer par les opérations d'information l'environnement informationnel des forces armées en OPEX, *Doctrine numéro spécial*, Les fonctions d'environnement, mai 2008

Chef du Groupement d'information Opérationnelle de la FAT, (2008), Les opérations militaires d'influence dans le cadre des opérations d'information, *Doctrine numéro spécial*, Les fonctions d'environnement, mai 2008

Combelles-Siegel, P., (2002), *Operational Communication And Multilateral Operations : A Comparison Of American, British And French Doctrines And Practices*, Fondation pour la recherche stratégique (FRS).

Huyghe, F.-B., (2001), *L'ennemi à l'ère numérique, Chaos, information, domination*, PUF, Paris.

Ministère de la da défense (2008), *La manoeuvre globale*, Centre de doctrine d'emploi des forces

BPR: Opérations d'information du J6 (1998), *Opérations d'information des FC*, Publiée avec l'autorisation du Chef d'état-major de la Défense, B-GG-005-004/AF-010, Défense nationale canadienne.

Behelf für Generalstabsoffiziere (BGO10), Behelf 52.070 d, Stand Januar 2009

Conduite tactique XXI, Règlement 51.020 f, 2004

Conduite opérative XXI, Règlement 51.070 f, 2004

Commandement et organisation des

états-majors de l'armée, Règlement 52.054 f, 2004

Etude conceptuelle Information Operations (KS IO), janvier 2005

Présentation du Colonel EMG Vernez, G., InfoOps, 2007

Standartprozesse für Informationsoperationen, Beitrag zur Revision des BGO, septembre 2008