Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2007)
Heft: 3

Artikel: Les opérations d'information dans l'armée suisse
Autor: Vernez, Gérald
DOI: https://doi.org/10.5169/seals-346707

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 06.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Source de l'assemblage d'images L. Monnerat

Les opérations d'information dans l'armée suisse

Col EMG Gérald Vernez

EM cond A, J35, chef des opérations d'information.

Quelle menace justifie une telle capacité? Combien cela va-t-il coûter? Qu'est-ce que cela va rapporter? N'est-on pas simplement en train de recopier ce que font les autres? Une telle capacité est-elle acceptable, politiquement, juridiquement, moralement, éthiquement?

Voilà une série - non exhaustive - de questions et d'objections latentes pouvant découler de ce titre et auxquelles le présent article ambitionne de donner une première réponse au moyen de 6 tableaux. Auparavant, il convient de souligner à quel point ce domaine est sensible et complexe et à quel point il est important de prendre notre temps pour faire les choses justes, de ne pas condamner a priori, ni, non plus, de voir là l'arme absolue face à tous les maux modernes. C'est une corde de plus à notre arc sécuritaire, ni plus ni moins.

Un peu de recul

Pour comprendre les opérations d'information (InfoOps) il est utile de remonter au général chinois Sun Tzu et son *Art de la Guerre*. Quand on sait le prix des conflits, pour soi-même comme pour l'ennemi, on ne peut en effet pas rester insensible à un principe tel que « le bon général a gagné la bataille avant de l'engager ».

Nombreux sont ceux qui reprochent à Sun Tzu de n'avoir jamais gagné de bataille, d'avoir emprunté ses idées à son oncle, ou encore de n'avoir fait que de philosopher. Pour les barbares qui ont conduit la guerre pendant les 25 siècles suivants, quoi de pire qu'un général qui vous dit « l'art de la guerre, c'est de soumettre l'ennemi sans combat ». A ce train là, nos livres d'histoire auraient cruellement manqué de cadavres!

Mais que serait devenu le monde si l'on avait tenté, chaque fois que cela était possible, de faire la guerre, comme le suggère Sun Tzu, avec d'autres moyens et par d'autres chemins. Car la force et la destruction ne sont pas tout. Quand Clausewitz écrit « la guerre n'est qu'un prolongement de la politique par d'autres moyens », cela ne signifie pas que le retour d'ambassadeurs bredouilles doit déclencher immédiatement l'emploi de la canonnière. Derrière son concept de « guerre totale », il n'a pas prétendu qu'il fallait anéantir l'ennemi et tout son pays. Au contraire, il entendait par là, qu'entre la politique et la guerre il y a de nombreux autres moyens de soumettre l'adversaire. Aujourd'hui, les opérations d'information en font partie.

Origines et caractéristiques des InfoOps modernes

Lorsque l'on considère individuellement les méthodes mises en œuvre dans le cadre des InfoOps, on peut avoir le sentiment qu'il n'y a absolument rien de nouveau. En revanche, considérées globalement et en appréciant leurs effets potentiels, on doit admettre au contraire qu'il s'agit véritablement d'une nouvelle capacité.

Ne rien faire pour maîtriser la dimension informationnelle dont elle entend se charger reviendrait à l'abandonner complètement à l'adversaire. Les conséquences seraient telles, que l'usage « normal » du solde des moyens terrestres et aériens classiques pourrait devenir impossible (que faire si plus aucun système ne fonctionne et plus personne ne veut servir) ou vain (s'il y a déjà eu défaite sur le plan stratégique, quelle serait l'utilité d'un déploiement militaire).

Sous sa forme moderne et intégrale, la théorie de base des InfoOps provient majoritairement des USA. C'est à travers les travaux d'auteurs tels que Libicki ou Arquilla & Ronfeldt que la notion de « guerre de l'information » (ou *Information Warfare*, IW) est devenue populaire. Vers 1995, l'armée américaine a ensuite publié ses premiers règlements au sujet des IO ou *Information Operations* (FM 3-13, JP 3-13, AFDD 2-5) où l'on précisait « *IW is IO during time of war or crisis* », suggérant ainsi sans équivoque que dans l'esprit des décideurs américains, les InfoOps sont un moyen utilisable en temps de paix déjà.

Les raisons pour lesquelles les USA ont joué un tel rôle dans la diffusion de ce domaine sont multiples. Sans chercher à être exhaustif, on peut citer:

- leur expérience de guerre continue depuis plus de 150 ans et, surtout depuis la Seconde Guerre mondiale, un investissement massif, cohérent et systématique dans la recherche (technique et doctrinale) pour conserver leur avance;
- l'analyse systématique de leurs actions et la publication de ces résultats par de nombreux canaux, tant militaires qu'académiques ou politiques, notamment par le GAO - General Accountability Office - bras armé du Congrès américain pour la vérification de l'emploi des fonds publiques;

- leur domination dans les cénacles internationaux au travers de l'émergence d'une « science internationale de la défense », que ce soit dans le cadre européen de l'OTAN, celui de l'ONU pour la maîtrise des conflits, lutte anti-terrorisme compris;
- leur investissement dans les technologies de l'information qui les a placés dans une position très dominante, puisqu'il n'est pas un pan de nos sociétés qui ne parvienne à échapper à leur influence ou à celle de leur industrie.

Pour des raisons de langue et de domination doctrinale, l'école russe est quant à elle pour ainsi dire inconnue. On sait toutefois que les premières publications venues des USA sur la guerre de l'information ont entraîné des réactions très vives. Ainsi, démunie face à de probables attaques via le cyberespace, l'armée russe a même laissé entendre durant les années 90 que si elle avait à subir de telles actions, la gravité serait telle qu'elle légitimerait l'emploi de l'arme nucléaire. Comme tout le monde, les russes travaillent sur le sujet; qu'ils structurent ou non leur doctrine comme l'Occident n'est pas significatif; dès lors qu'ils disposent de tous les moyens nécessaires pour conduire des InfoOps et qu'ils sont même des maîtres dans certains domaine. L'emploi qu'ils feront de l'espace informationnel ne dépendra que de leurs objectifs stratégiques. A cet égard, le durcissement actuel de leurs positions n'est certainement pas réjouissant.

Avec la Chine, la barrière linguistique est encore plus forte et l'accessibilité à ce qui s'y fait encore plus réduite qu'en Russie. Mais, là aussi, moyens et histoire ne laissent aucun doute sur l'intention de faire un usage complet de toute la panoplie de moyens et méthodes que nous reconnaissons comme *InfoOps-relevant*. De nombreux événements récents dans le cyberespace, attribués à la Chine, ou ne serait-ce que tolérés par celle-ci, conduisent même un nombre croissant d'experts à tirer la sonnette d'alarme. L'Occident ne semble pas encore bien comprendre l'énormité des efforts de modernisation entrepris par la Chine, où les InfoOps jouent un rôle croissant. Certains auteurs font même état de troupes opérationnelles en matière de cyber-guerre; celles-ci auraient déjà été récemment engagées avec succès lors de grandes manœuvres.

La Chine développe aussi depuis 10 ans des concepts dans le domaine du *Unrestricted Warfare* et des *Non-Military War Operations*. Ces théories parlent de l'usage de la guerre financière, commerciale ou encore des ressources. Elles s'étendent même jusqu'à l'instrumentalisation du champ juridique international et du commerce de la drogue en tant que moyens. Leur application vise clairement à mettre des sociétés à genoux et, dès lors qu'une telle stratégie (que de nombreux acteurs peuvent d'ailleurs utiliser) atteindrait ses objectifs contre un Etat comme le nôtre, on peut légitimement se demander si ce dernier disposerait du ressort suffisant et des opportunités pour engager des moyens militaires? Mais avant cela, il faudra acquérir des preuves contre le coupable, qui seront en mesure de justifier notre action. Et que faire s'il se trouve de l'autre côté du globe ?

S'agissant de la nébuleuse terroriste, l'usage toujours plus important de l'infosphère pour communiquer, conduire, instruire et recruter, est démontré et d'échelle mondiale. Mais c'est surtout en matière de gestion des perceptions que la maîtrise des terroristes est la plus éclatante. Ainsi, le 11 septembre 2001 doit-il être vu moins comme œuvre de destruction qu'en tant que gigantesque provocation parvenue à compromettre les USA dans des conflits où finalement, en moins de 4 ans, ils se seront aliénés une part importante du soutien et du respect dont ils jouissaient auparavant. La victoire militaire n'implique pas une victoire stratégique ou médiatique. C'est même ici clairement l'inverse, d'autant que les USA auront été ainsi forcés à dépenser des centaines de milliards, avec à la clé un déficit budgétaire record, sans compter les autres séries de conséquences.
L'objet de ces exemples n'est bien sûr pas de comparer la Suisse à ces géants ou à des nébuleuses hors de notre portée.

En revanche, la lecture des faits, leur expérience opérationnelle, leurs efforts de développement doivent nous aider à comprendre les conséquences d'un usage bien compris des InfoOps:

- on voit clairement l'ouverture d'un nouveau « front » impliquant que la domination en termes de moyens et de force brute n'est plus suffisante pour gagner; la maîtrise de l'infosphère peut même avoir une importance supérieure; certaines méthodes peu onéreuses des InfoOps peuvent permettre d'obtenir des effets très importants relativement à leur coût, les rendant attractives et à la portée de n'importe qui;
- les frontières ne nous protègent plus; une action peut être lancée n'importe quand, sans délai d'alerte et depuis n'importe où; le concept de profondeur opérative devient inopérant; en terme de renseignement, les intentions de l'adversaire sont plus importantes que la nature de ses moyens;
- une action dans l'infosphère est le plus souvent indétectable; en conséquence, même un ami peut en faire usage et lorsqu'il deviendra évident que quelque chose s'est passé, la paternité de l'action a toutes les chances de rester inconnue; la notion de « seuil des hostilités » perd donc de sa signification, puisqu'une part importante des actions se déroule en temps de paix déjà.

Compréhension doctrinale des InfoOps en Suisse

Les premiers travaux ont été lancés dans notre pays en 1996. Malheureusement, axés presque uniquement sur l'environnement cybernétique, ils se sont rapidement arrêtés. Le groupe des opérations de l'Etat-major général s'est alors saisi du dossier pour réaliser une étude préliminaire qui a permis, fin 2001, de justifier la réalisation de travaux conséquents et d'en définir le cadre. Sur cette base a ensuite été réalisée une étude conceptuelle approuvée début 2005. Comme certains l'avaient suggéré initialement, on aurait pu se contenter de recopier la doctrine américaine, de loin la plus complète et la plus aboutie. L'analyse a cependant rapidement démontré que cela n'était pas possible, en raison des différences importantes qui nous distinguent des USA en matière de culture, de stratégie, de bases légales, de morale, de moyens, etc.. De plus, comme la plupart des doctrines étrangères, celle des USA est tournée vers un emploi des forces à l'extérieur de leurs frontières, alors que nos missions sont axées sur la défense du territoire. La défense implique que les effets créés par notre armée concernent en même temps nos adversaires et notre propre population. Les exemples de l'Afghanistan ou de l'Iraq nous aident peu pour développer le métier dont nous avons besoin.

Notre doctrine, actuellement en cours de finalisation, est donc un produit complètement en phase avec nos moyens, nos besoins et nos caractéristiques. Bien qu'originale, notre démarche n'a pas pour objectif de se distancer absolument de tout ce que les autres pays ont appris, parfois au prix de la vie de leurs soldats, mais de s'assurer que ce que nous faisons est juste, justifié et que nous sommes en mesure d'en expliquer tout le contenu.

Durant nos travaux, nous avons vécu des étapes importantes, telle que l'opération mise sur pieds pour le passage à l'an 2000 (opération MILLENNIUM TRANSIT), où des constats essentiels sur la relation entre l'information et l'acte de gouverner, ou encore en matière d'infrastructures critiques, ont été faits.

Mais ce sont surtout l'étude de base sur le système de conduite de l'Armée XXI et la rédaction du règlement qui en a découlé (Commandement et organisation des états-majors de l'armée - COEM XXI) qui ont joué un rôle clé dans le développement des InfoOps. Ces travaux ont en effet permis de mettre en évidence quelque chose qui n'est trivial qu'en apparence: toute action est le résultat d'un processus de décision.

Qu'il s'agisse de lever un bras pour se protéger les yeux d'une lumière aveuglante ou pour réaliser le débarquement de Normandie, il faut désigner un objectif, déterminer les paramètres opérationnels (espace, forces, temps, information), trouver des solutions, planifier, synchroniser, ordonner, contrôler et, cas échéant, corriger. Empêcher au processus de prise de décision de fonctionner revient donc à empêcher l'action qui en dépend. On comprend à travers cet énoncé, que l'on peut concevoir de gagner autrement qu'en opposant à la force adverse une force équivalente ou supérieure: c'est-à-dire de ne pas entrer dans une logique d'escalade.

Pris sous cet angle, les InfoOps sont une formidable opportunité de mener la bataille de manière non létale, d'être vainqueur sans devoir tout reconstruire, d'éviter la création d'un nombre infini de veuves et d'orphelins (donc autant d'ennemis supplémentaires, aussi dans nos propres rangs) à qui il faudrait autrement expliquer pourquoi leurs parents sont morts au combat.

Pour un pays comme le nôtre, dont les ressources sont réduites, une telle approche, aussi appelée « du faible au fort », peut donc s'avérer dans de nombreuses situations largement plus payante que le combat d'usure. Cette stratégie n'exclut toutefois d'aucune façon les autres méthodes et il reste indispensable de disposer de moyens lourds en suffisance.

Sur la base de ce qui précède, la définition des InfoOps que nous appliquons en Suisse est la suivante: « Ensemble des mesures appuyées par le renseignement et ayant pour but d'influencer, perturber 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. »

Explication de notre doctrine et mise en œuvre pratique

Pour la mise en œuvre de la définition qui précède, on travail selon le principe « objectif - méthode – moyens » [1].

Cela revient aussi à dire que la stratégie d'emploi des InfoOps est basée sur les effets[2]. 8 méthodes principales ont été identifiées, ainsi qu'un nombre important de sous-méthodes.

S'agissant des moyens, leur nombre et leur nature ne sont pas des facteurs déterminants, car ils changent très souvent en fonction des progrès techniques et leur disponibilité est variable. Au moment voulu, on sélectionnera donc dans la « boîte à outils » les moyens permettant de délivrer les effets escomptés.

Ce n'est donc pas le contenu de la boîte à outil qui nous dicte nos objectifs, comme cela est encore trop souvent le cas !

La quasi-totalité de ces méthodes sont bien sûr connues, certaines même depuis Sun Tzu. Ce qui est en revanche nouveau et qui rend les InfoOps intéressantes et efficaces, c'est l'emploi coordonné de toutes ces méthodes afin de maîtriser cet indispensable champ opérationnel qu'est devenue la sphère informationnelle, du fait de l'explosion de la signification des médias et de la technologie de l'information.

1 *End - Way - Means*
2 EBO: Effect Based Operations.

Développement et usage opérationnel des InfoOps

Par définition, les InfoOps peuvent être conduites seules: on les qualifie alors de *Standalone*. Les InfoOps peuvent avoir besoin des effets d'autres lignes d'opération (on parle alors de *Supported*), ou appuyer ceux-ci (on dira alors qu'elles sont *Supportive*). Le plus souvent, la taille du domaine informationnel sera quasi illimitée, au contraire d'une unité tactique disposant de limites de secteur claires. Le grand nombre d'acteurs à considérer qui en découle, aura pour conséquence un travail considérable et complexe de planification et de synchronisation.

La partie conceptuelle est approuvée depuis 2005, mais il ne s'agit que de théorie et le plus dur reste à faire: rendre opérationnelles ces théories. Avant d'en arriver là, d'importants progrès sont encore nécessaires pour maîtriser et délimiter ce nouveau métier. En effet, il est impératif de considérer les contraintes politiques, légales, morales et éthiques auxquelles les InfoOps seront confrontées. La volonté des créateurs de cette capacité opérationnelle n'est pas de développer un « monstre » qui échappe à tout contrôle, mais bien de mettre dans les mains de notre pouvoir politique un outil supplémentaire qui lui permette de remplir ses missions constitutionnelles. Ce souci de rigueur a conduit, dès le début, les acteurs de ce dossier à se faire conseiller par des personnes du monde politique, économique et académique et à rendre public le travail effectué. Il est évident, dès lors que nous passerons dans le monde opérationnel, que ce sont les entités usuellement responsables du contrôle démocratique qui reprendront le flambeau. Pour l'instant, nous sommes dans la phase des essais où nous essayons aussi souvent que possible de pratiquer les InfoOps afin de mettre en évidence tous les obstacles et difficultés possibles. A cet effet, le personnel de la section des InfoOps de l'Etat-major de conduite de l'armée a participé ces dernières années, tant sur le plan national qu'international, à de nombreux exercices de l'échelon brigade à l'échelon armée, de fréquents échanges d'idées avec d'autres experts lors de séminaires et conférences. Tous les enseignements tirés servent à affiner la doctrine et à déterminer avec la plus grande précision possible quels moyens devront être mis en œuvre. Dans un cas de sécurité sectorielle, le gain escompté pourrait dans la durée s'exprimer notamment à travers:

- le soutien de la volonté de défense de la nation (aussi par des activités visant à contrer la démission ou le défaitisme entretenu par l'adversaire) et la projection univoque des intentions du peuple Suisse à ses partenaires comme à ses adversaires;
- toute action permettant d'éviter des affrontements entre groupes antagonistes et donc épargner des victimes et économiser des engagements inutiles de nos forces;
- la sensibilisation de divers publics par rapport à toutes sortes de dangers, afin de diminuer les risques d'accidents et de lésions;
- la participation à la protection d'entités (personnes, symboles, etc.) et d'infrastructures essentielles à la nation et à la mission de l'armée;
- l'évaluation de nos mesures de protection, afin de déceler à temps des failles exploitables par un adversaire contre notre processus décisionnel;
- la participation à l'amélioration de notre propre processus décisionnel, afin d'améliorer la fluidité, la précision et la rapidité des actions (aussi avec les partenaires civils) et ainsi contribuer à la réduction des coûts opérationnels;
- des mesures actives contre le processus de décision de nos adversaires en cas d'escalade, afin de les empêcher d'agir contre nous ou de réduire leur efficacité;
- la contribution durable à la désescalade à l'issue d'une crise, afin de désengager les moyens lourds dès que possible et éviter une réactivation du conflit.

Conclusion

L'information a toujours aidé à façonner les conflits. Il serait naïf de ne pas le reconnaître et intellectuellement inacceptable de passer sous silence ses excès. Se passer de la capacité de tenir notre rang dans l'espace informationnel reviendrait tout simplement à:

- abandonner un domaine opérationnel complet à l'adversaire, ou il pourra ensuite agir à sa guise contre notre armée et contre notre société;
- renoncer à la capacité de déchiffrer les actions de nos adversaires, de déjouer leurs plans et de leur appliquer des contre-mesures adéquates;
- renoncer à un moyen non létal et bon marché de remporter des succès; qui souhaite aller annoncer aux familles, « nous avons préféré nous battre contre l'ennemi plutôt que d'essayer de désactiver ses armes ou de l'influencer pour qu'il renonce au combat; votre fils en est mort, ... désolé »? Il n'est bien sûr pas question ici de la doctrine utopiste de « zéro mort », mais d'une façon permettant de réduire les pertes de tous les côtés.

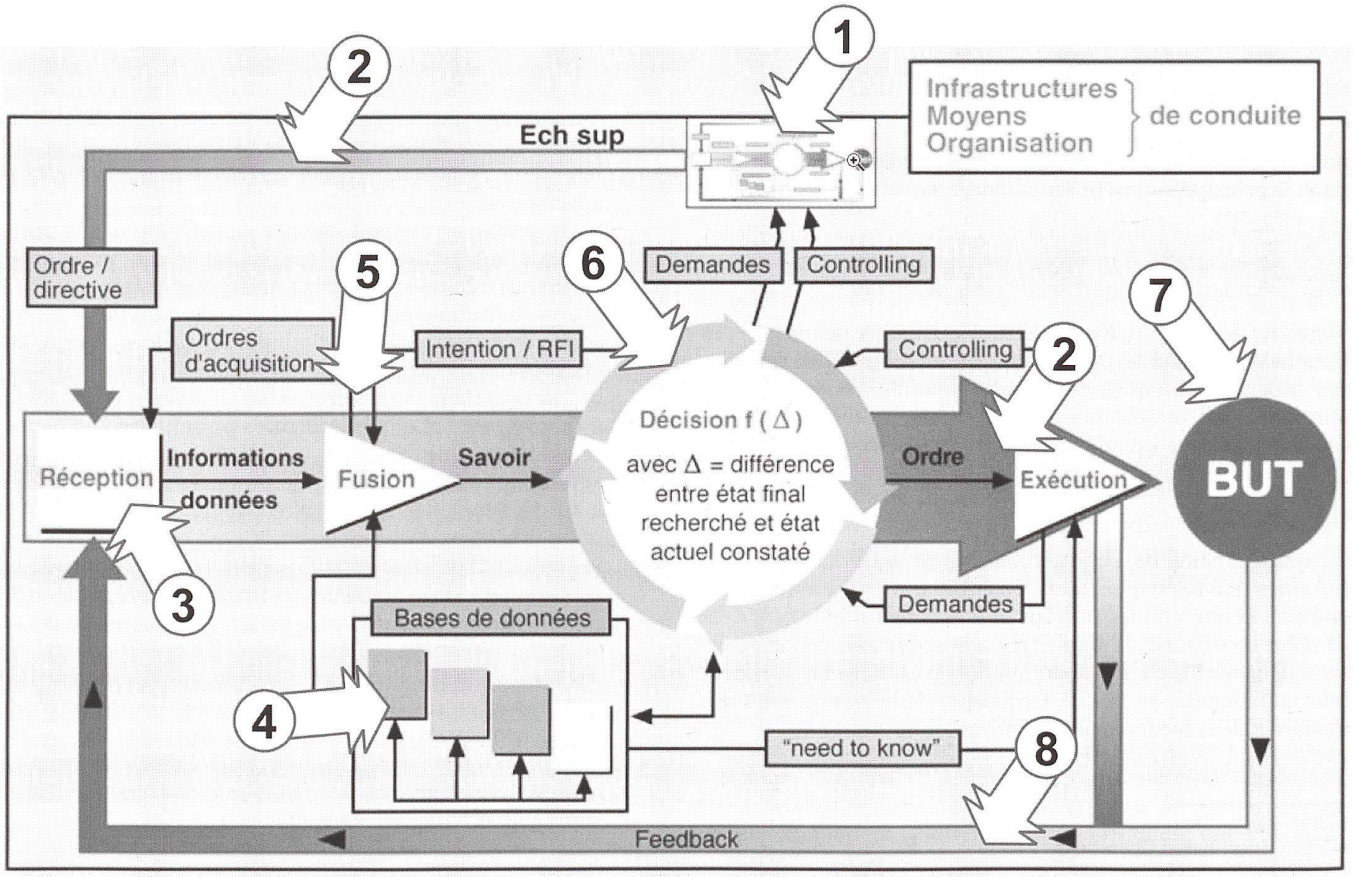
En matière de contenu, la Suisse est arrivée à un très bon niveau qualitatif. En revanche, sur le plan quantitatif, elle peine à trouver les ressources nécessaires, ne serait-ce que pour piloter les quelques chantiers indispensables à la phase de développement et des essais. Les InfoOps sont d'une grande complexité et moins nous disposerons de moyens, plus il faudra de temps pour les mettre en œuvre. La conduite et la synchronisation sont donc des éléments clé et une telle fonction est aussi à l'étude pour l'échelon stratégique.
En effet, celui-ci doit obligatoirement et dès que possible intégrer cette dimension dans ses prises de décisions pour tous les types de crises. Il est un dicton chez les Israéliens, dont nous devrions nous inspirer: « faisons ce qui est compliqué pendant que c'est facile » et un autre que l'on pourrait attribuer aux comptables: « *faisons d'abord ce qui est efficace et bon marché* ».

G.V.

Des réflexions futuristes

La figure suivante, issue de la COEM XXI, montre que le processus décisionnel se compose d'infrastructures, de moyens technologiques, d'organisations (donc de personnes) et d'informations. Les flèches ajoutées sur la figure originale démontrent comment les InfoOps peuvent s'attaquer au processus décisionnel:

1. perturber le fonctionnement d'un échelon de commandement revient à perturber celui de ses subordonnés;
2. empêcher ou perturber la transmission d'ordres ou de données revient à ralentir le processus ou à empêcher sa mise en route; pas d'ordre = pas d'action; faux ordre = fausse action;
3. perturber le fonctionnement des senseurs revient à ne pas disposer des bons renseignements pour travailler; faire livrer de fausses informations par les senseurs, c'est s'assurer que toute l'action prendra une direction erronée, ne se déroulera pas à temps, ou que l'on ne reconnaîtra même pas la nécessité d'agir;
4. aller dans les bases de données et fausser des données ou les faire disparaître empêchera de faire des recoupements et des vérifications et entraînera de fausses décisions;
5. éliminer ou perturber le travail des instruments et du personnel nécessaire à l'établissement du savoir va ralentir ou empêcher une décision rationnelle;
6. éliminer le commandant, donc le décideur, couper l'électricité, griller les ordinateurs de l'état-major, c'est empêcher de prendre une décision et de la formaliser; menacer une personne clé de représailles contre sa famille s'il persiste à son poste ou s'il refuse de saboter celui des autres revient aussi à empêcher le fonctionnement de la prise de décision;
7. faire en sorte que le mauvais objectif soit désigné, par des mesures de camouflage ou de déception, c'est envoyer à coup sûr l'adversaire dans la mauvaise direction;
8. s'assurer que le retour d'information du front livre des données inexactes ou fausses, ... et on revient au cas numéro 3.



Le tableau présente les caractéristiques des méthodes principales mises en œuvre dans le cadre des InfoOps pour influencer, perturber, détruire le processus décisionnel adverse, tout en protégeant et améliorant notre propre processus décisionnel

Méthode	Caractéristiques et effets	Principales sous-méthodes
Renseignement	Ensemble des processus par lesquels l'information est acquise, analysée, fusionnée et stockée afin d'être transformée en savoir au profit des InfoOps. Il recouvre par conséquent les méthodes classiques des organes du renseignement sans lesquels les InfoOps seraient totalement inopérantes. Les besoins des InfoOps posent cependant au renseignement des exigences nouvelles.	Exploration des signaux (SIGINT). Renseignement technique (TECHINT). Renseignement par mesures et signatures (MASINT). Contre-renseignement (CI). Renseignement humain (HUMINT). Renseignement de sources ouvertes (OSINT). Gestion des connaissances (KM, knowledge management).
Opérations des réseaux informatiques (CNO = Computer Network Operations)	Ensemble des activités offensives et défensives en rapport avec les systèmes informatiques (donc dédiés à l'acquisition, au traitement, au stockage, au transport et à la représentation de données sous forme digitale).	Attaques de réseaux informatiques (CNA) afin de perturber ou détruire la fonctionnalité de réseaux en visant tous les équipements et leur contenu informationnel et fonctionnel. Exploitation de réseaux informatiques (CNE) afin d'acquérir du renseignement avec les mêmes méthodes que le CNA, mais sans faire de dégâts. Défense de réseaux informatiques (CND); le CND est une défense dynamique des réseaux et de l'infrastructure informatique et donc un complément à la sécurité informatique (COMPUSEC).
Sûreté de l'information (IA = Information Assurance)	IA désigne l'ensemble des mesures servant à la sécurisation et à la protection des informations sensibles afin d'assurer leur intégrité lors de l'utilisation.	Sécurité informatique (COMPUSEC), afin d'empêcher l'accès à des utilisateurs non autorisés (défense statique de l'infrastructure informatique). Sécurité des émissions (EMSEC) afin d'éviter que des émissions secondaires des systèmes soient exploitées. Sécurité des communications (COMSEC) afin que les contenus captés ne puissent être déchiffrés. Protection des infrastructures d'information critiques (CIIP); ce domaine a une dimension interdépartementale forte et des liaisons avec le monde civil et privé.
Sécurité des opérations (OPSEC = operations security)	Ensemble des contre-mesures (on peut parler de Counter-OSINT) prises pour empêcher que des informations (pour la plupart non classifiées et appelées « indicateurs ») ne permettent à l'adversaire d'accéder par reconstruction à des informations classifiées ou lui permettant d'agir contre notre processus décisionnel.	Protection des personnes (PERSSEC: Personal Security). Classification des informations. Camouflage afin de protéger de l'observation nos capacités et intentions. Déception afin de tromper l'adversaire sur nos intentions réelles.Protection des infrastructures vitales (CIP : Critical Infrastructure Protection).
Opérations basées sur les réseaux (NEO = Network Enabled Operations)	Afin de disposer dans l'exécution d'une plus grande précision et d'une rapidité accrue afin de prendre l'avantage sur l'adversaire et d'économiser nos forces, il s'agit d'améliorer nos processus et de développer une véritable culture du travail avec l'information.	Instruction et entraînement des forces et des décideurs. Intégration et interopérabilité des composantes des forces. Systèmes de communication et d'information nécessaires au commandement et au contrôle.
Conduite de l'information opérationnelle (cond info op, aussi appelé PSYOPS dans le milieu international)	Sont comprises ici toutes les activités visant à influencer les perceptions, l'attitude et le comportement d'une audience définie. Etant donné que les vecteurs principaux de l'information publique sont les médias, des règles strictes doivent être édictées pour que ceux-ci ne soient directement instrumentalisés, surtout en ce qui concernerait la propagation de fausses informations.	Communication : donner du sens avec des perceptions vraies pour obtenir l'adhésion d'une audience cible; comprend l'information, la coopération et la persuasion. Mystification : altération du sens (modification du jugement) d'une audience cible par la diffusion de perceptions orientées (vraies), fausses ou fictives afin de l'amener à prendre des décisions défavorables à sa cause; comprend la désinformation, la fiction et la publicité (pendant civil du terme propagande). Aliénation (exclu des actions envisageables par une démocratie et mentionné uniquement pour mémoire en tant que menace): imposition d'un sens à une audience cible en l'obligeant à accepter des perceptions fausses; comprend le contrôle psychologique et le terrorisme.
Effets physiques	Usage de tout moyen capable de créer des effets cinétiques contre une partie du processus décisionnel. De tels effets peuvent avoir un but perturbateur, destructeur, mais aussi d'influence (un déploiement de moyens lourds sert avant tout à impressionner !).	Actions de contact ou distantes (avec ou non destruction cinétique).Armes non létales (NLW, non lethal weapons) antipersonnel et antimatériel. Armes à énergie dirigée (DEW, directed energy weapons). Armes à énergie non dirigée (NDEW, non directed energy weapons).
Combat électronique (EW = electronic warfare)	Combat pour l'utilisation du spectre électromagnétique.	Contre-mesures électroniques (ECM, electronic counter-measures). Mesures d'appui électroniques (ESM, electronic support measures). Mesures de protection électroniques (EPM, electronic protective measures).