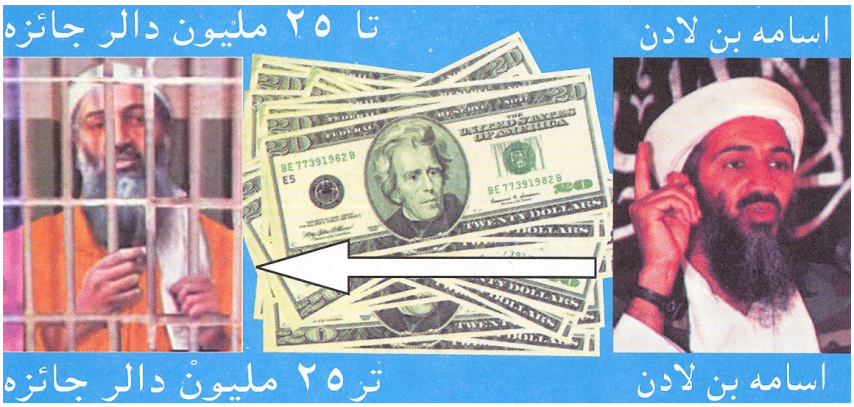
Politique de sécurité: **analyses du CSS**

CSS ETH Zurich

N° 34 • mai 2008 • 3ème année

OPERATIONS D'INFORMATION: TENDANCES ET CONTROVERSES

Les opérations d'information ont gagné en importance ces dernières années. Influencer l'information d'un adversaire ou l'attitude de la population civile dans les secteurs d'intervention et sécuriser l'information et les systèmes d'information propres sont devenus des facteurs de réussite importants des opérations militaires. Ce concept a cependant donné lieu à de vives controverses. Il n'y a en effet aucun consensus quant au type de missions que les forces armées des Etats démocratiques peuvent et doivent réaliser ni quant à l'ampleur de ces missions. Il reste également à éclaircir la répartition des responsabilités et des tâches au niveau de l'interface civilo-militaire.



Tract américain utilisé en Afghanistan *psywarrior.com*

Le facteur information est depuis toujours un composant important du pouvoir, de la diplomatie et de la guerre. Sun Tzu, stratège chinois (env. 400–320 av. J.-C.), était déjà d'avis qu'il était indispensable au guerrier de connaître son adversaire et ses propres forces d'anéantissement pour remporter la bataille et que la supériorité informationnelle permettait même de remporter des guerres sans combat. Mais, même si l'histoire de la guerre de l'information est aussi vieille que l'art de la guerre, ce n'est que depuis récemment que des moyens permettant d'influencer complètement l'adversaire par l'information sont disponibles, ce qui explique le regain d'importance qu'a connu ces dernières années l'information comme élément d'une politique de sécurité et de défense efficace.

Le concept des «Information Operations» (Info Ops) a été développé par les Etats-Unis dans les années 1990 et intégré à la doctrine militaire nationale. Ce concept regroupe les principes éprouvés des stratégies informationnelles traditionnelles et prolonge dans ce sens les objectifs de la politique d'information classique en temps de guerre. Mais il introduit en outre de nouveaux éléments importants. En particulier, la souveraineté de l'information ne s'entend plus comme un élément de soutien de la guerre mais comme une forme de combat en soi susceptible d'avoir un effet décisif dans les conflits actuels. Les médias et les informations sont des instruments supplémentaires intégrés dans l'arsenal d'armes offensives et défensives. Le concept des opérations informationnelles modernes reflète et renforce le flou croissant entre les aspects militaires et non militaires de la politique de sécurité. Il nécessite simultanément une coordination élevée entre le niveau militaro-opérationnel et le niveau politico-stratégique ainsi qu'entre les acteurs étatiques et non étatiques.

Des composantes défensives et offensives

La production, la gestion et l'évaluation de l'information occupent désormais une place plus importante en raison des développements technologiques dans le domaine de l'information et de la communication ainsi que d'une utilisation très répandue de ces technologies dans tous les domaines de l'économie, de la politique et de la société. La maîtrise des nouvelles technologies et l'influence des contenus informationnels sont devenues une ressource centrale de pouvoir.

C'est principalement sur cette toile de fond qu'a été élaboré le concept des opérations d'information. La guerre du Golfe de 1991 passe d'ordinaire pour le début d'une nouvelle génération de guerres où ce n'est plus la violence physique mais la capacité de gagner la «guerre de l'information» et d'obtenir la «supériorité informationnelle» qui décide en premier lieu de la victoire. Si la discussion correspondante était, dans une première phase, étroitement concentrée sur le potentiel militaro-opérationnel des opérations d'information, les nombreux risques bien plus étendus liés à cette évolution n'ont quant à eux pas tardé à se manifester. Plus on active le débat autour des attaques contre les systèmes d'information d'éventuels adversaires, plus

on thématise la vulnérabilité comparativement élevée des propres réseaux de données militaires et civils. C'est pourquoi l'objectif défensif consistant à protéger la propre infrastructure critique de cyberattaques et d'autres risques est apparu vers le milieu des années 1990 en plus des composantes offensives des opérations informationnelles (cf. analyse du CSS n° 16). Les US Joint Chiefs of Staff ont formulé pour la première fois en 1998 une doctrine complète interarmées.

Aujourd'hui, on entend en règle générale par opérations d'information des activités militaires coordonnées dans le but d'exercer un effet recherché sur la volonté et la capacité de décision de troupes adverses et/ou l'attitude de la population civile dans les secteurs d'intervention et de protéger les propres informations et systèmes d'information. De telles opérations peuvent comprendre un vaste éventail d'instruments comme p.ex. les opérations psychologiques, la destruction physique, la guerre électronique, des attaques contre des réseaux informatiques et leur défense, la déception militaire, la contre-propagande, la sûreté de l'information, la sécurité des opérations et l'infiltration d'ordinateurs. Une comparaison des plus de 20 doctrines Info Ops existantes d'Etats et de l'OTAN fait cependant clairement ressortir les différentes manières dont est appliqué le concept. Tous les Etats ne disposent pas, loin s'en faut, de la volonté politique ou des capacités de mettre en œuvre toute la gamme d'instruments. La majorité des Etats donne aussi davantage de poids aux mesures défensives qu'à d'éventuelles actions offensives.

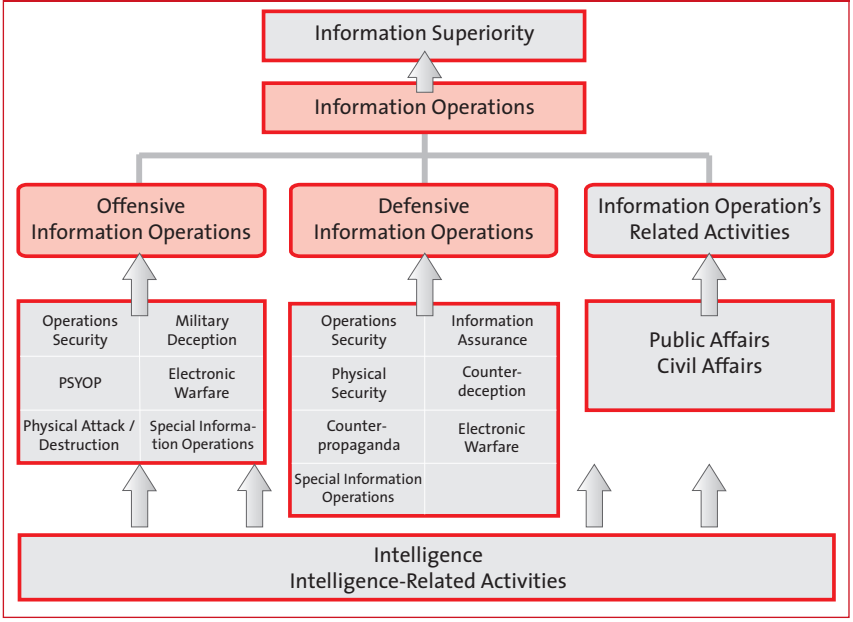
Une tâche transversale et commune

On peut, malgré cette hétérogénéité, identifier trois éléments caractéristiques des opérations d'information actuelles. Premièrement, ces opérations revêtent une fonction transversale dans l'éventail des types d'opérations militaires. Les opérations informationnelles jouent un rôle important tant dans l'opération défensive que dans les missions infraguerrières et les missions de stabilisation internationales. Alors que l'on n'a recours à une mesure comme le bombardement de stations radar qu'en cas de guerre, d'autres instruments sont quant à eux mis en œuvre dans tous les types d'opérations.

Deuxièmement, les opérations informationnelles ne doivent pas s'entendre de manière isolée comme une mission purement militaire mais comme faisant partie d'une tâche commune de l'armée et d'acteurs civils étatiques et non étatiques dans l'esprit d'une stratégie d'information complète. C'est ainsi que l'armée ne peut souvent apporter qu'une contribution limitée dans le domaine des opérations d'information défensives. Elle joue par exemple dans le cas de la protection d'infrastructures critiques un rôle subalterne qui se limite pour l'essentiel à la sécurisation de ses propres réseaux. La gestion des risques informatiques, c.-à-d. des attaques possibles d'acteurs étatiques ou non étatiques contre des systèmes et infrastructures informatiques, exige en premier lieu un partenariat étroit entre l'Etat et l'économie ainsi qu'une coopération interétatique intensive. Mais les risques d'information, c.-à-d. les risques qui ont trait au contenu de l'information, ressortent en premier lieu du domaine de la responsabilité politique. L'armée peut cependant apporter des contributions importantes, par exemple pour identifier la désinformation ennemie ou protéger les structures de direction nationales.

Dans d'autres domaines principalement offensifs des opérations informationnelles, le niveau militaire opérationnel et le niveau militaire tactique concernant la conduite et la réalisation des opérations d'information jouent à vrai dire souvent un rôle considérable. Mais ces opérations ont aussi souvent, sans mesures parallèles et coordonnées du niveau politico-stratégique, un effet limité. Elles manquent en outre fréquemment de légitimité (cf. ci-dessous). Le besoin de coopération et de coordination plurisectorielle augmente d'autant plus que ces opérations d'information ne ciblent plus souvent, aujourd'hui, des espaces et systèmes d'information clairement délimités géographiquement mais le grand public.

Opérations informationnelles selon la doctrine américaine (JP3-13)



Pleins feux sur les opérations psychologiques

Troisièmement, on peut, en se basant sur cette dernière observation, constater une importance croissante des opérations psychologiques (PSYOP) au sein des opérations informationnelles. Ces opérations sont des mesures visant à influencer le comportement et les attitudes des troupes ennemies et/ou de populations civiles étrangères dans le contexte d'opérations militaires. Leur importance croissante s'explique d'une part par la menace du terrorisme international qui exige, du point de vue des Etats, des contre-mesures complètes également dans le domaine de l'information. Il faut comprendre le terrorisme non pas comme une méthode de guerre asymétrique seulement mais aussi comme une stratégie de communication. Grâce aux moyens de communication modernes, les terroristes peuvent diffuser sans grand effort leurs messages dans le monde entier. C'est pourquoi influencer positivement le public islamique et convaincre le public propre de la nécessité de lutter contre le terrorisme sont des pierres d'angle de la stratégie antiterrorisme occidentale. D'autre part, les expériences dans le domaine des missions de stabilisation multilatérales dans les territoires en conflit ces dernières années ont fait reconnaître l'importance éminente des opérations psy-

chologiques. Sans l'acceptation de la population locale, de telles missions sont vouées à l'échec à long terme, et c'est pourquoi la transmission et le contrôle de l'information par des programmes de radio, tracts, sites Internet, etc., jouissent d'une attention croissante

.

Mais les Etats appliquent aussi PSYOP différemment. La Bundeswehr allemande (qui parle d'information opérationnelle au lieu de PSYOP) prétend par exemple ne pas répandre d'informations fausses et influencer les opinions tout au plus par de l'information sélective. Dans la doctrine américaine par contre, les informations fausses délibérées sont elles aussi prévues comme faisant partie de la communication d'influence. La «propagande blanche», c'est-à-dire de l'information aussi factuelle et véridique que possible, doit par exemple, au ministère américain des affaires étrangères, être transmise sous le titre de «Public Diplomacy». On entend par ce terme un mélange de propagande étrangère, de marketing politique et de diplomatie culturelle. La «propagande noire», c.-à-d. la désinformation et la «propagande de démoralisation», a été institutionnalisée au ministère de la défense américain par l'«Office of Strategic Influence» en 2002. Même si ce bureau a été fermé en réponse aux protestations internationales, les forces armées américaines continuent de ne pas exclure explicitement l'utilisation de la désinformation. La Maison Blanche a en outre créé depuis un «Office of Global Communications» qui remplit des tâches similaires et dont le but est de coordonner toute la propagande étrangère des Etats-Unis. Il faut ajouter que les Etats-Unis misent souvent sur la «propagande grise», c.-à-d. sur des informations délibérément ambivalentes qui ne sont ni vraies ni fausses mais fixent un champ d'interprétation donné.

Besoin d'éclaircissements

Même si l'importance des opérations informationnelles a fortement augmenté ces dernières années, le concept reste entouré de controverses, surtout, du point de vue des Etats démocratiques, au niveau de la dimension offensive de ces opérations. Il s'agit ici d'éclaircir des questions fondamentales avant de bâtir d'éventuelles aptitudes.

C'est ainsi qu'il faut définir à quels aspects concrets des opérations informationnelles un Etat de droit peut légitimement avoir recours, et ce, dans quelle situation et dans quelle étendue. Une exclusion de principe des activités offensives ne convient pas, d'autant plus que, par exemple, les opérations psychologiques jouent, comme nous l'avons expliqué, un rôle de plus en plus important dans la réussite des opérations de paix multinationales. Mais dans quels contextes un Etat peut-il et doit-il manier par exemple la désinformation?

Des éclaircissements sont aussi nécessaires quant à la répartition des rôles entre l'armée et les autorités politiques. La question de savoir dans quelle mesure les forces armées doivent et peuvent se charger de tâches dans le domaine des opérations d'information offensives se pose en particulier ici. Il faudrait aussi examiner comment le contrôle et la conduite politiques de ces opérations militaires pourraient le cas échéant être garantis au niveau politico-stratégique. Il convient très généralement d'éclaircir les exigences posées au développement doctrinal et à la formation du personnel militaire dans le domaine des opérations d'information.

«Les opérations psychologiques devraient continuer de gagner en importance pour la Suisse»

Importance pour la Suisse

En Suisse aussi, le maniement de l'information en politique de sécurité est devenu un thème important. C'est ainsi que plusieurs offices fédéraux se penchent sur la sécurité de l'information, comme p.ex. l'Unité de stratégie informatique de la Confédération, le Service national de coordination de la lutte contre la criminalité sur Internet et la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI). Un examen général des risques et des contre-mesures à l'échelle fédérale est cependant absent. Le Conseil fédéral a, à la mi-2005, chargé l'Office fédéral de la protection de la population d'identifier avec tous les départements concernés le besoin d'action dans le domaine des infrastructures critiques et d'élaborer des mesures correspondantes. Une attention particulière devait être accordée aux risques de la société de l'information.

Dans l'armée, l'étude conceptuelle «Information Operations», qui donne une image complète des risques, dangers et chances de l'utilisation d'informations et de systèmes d'information en temps de guerre et de crise, a été clôturée en 2005 après de longs travaux. Les conclusions de cette étude ont entraîné plusieurs requêtes dans les domaines de l'organisation, de la doctrine et de la formation. Mais jusqu'à présent, seuls des éléments de conduite correspondants ont été créés au niveau de l'armée. La mise sur pied d'une fraction de l'état-major de l'armée pour la «conduite opérationnelle de l'information», c.-à-d. pour les opérations psychologiques, a, en été 2007, été remise à plus tard en raison d'ambiguïtés dans le domaine juridique, doctrinal et financier.

La Suisse a manifestement des problèmes avec les opérations d'information. Cela n'est pas étonnant puisque l'on peut observer des développements similaires dans d'autres Etats européens. La répartition des compétences au niveau des interfaces civilo-militaires des opérations informationnelles représente un défi particulier pour la Suisse. Du côté politique, les tâches de l'armée dans le domaine de l'information suscitent un certain scepticisme. Mais les menaces et risques probables aujourd'hui ne permettent guère de jeter forfaitairement le concept des opérations d'information pardessus bord. Il convient davantage d'examiner dans le détail dans quels domaines l'armée doit apporter des contributions et développer des aptitudes correspondantes. Les opérations psychologiques devraient continuer de gagner en importance pour remplir les mandats de l'armée. Des consignes politiques claires seraient cependant indispensables ici car, par exemple, la réaction à la désinformation relève indiscutablement du domaine de responsabilité des décideurs politiques.

Il faudrait s'efforcer d'incorporer conceptuellement les opérations d'information dans une stratégie globale de l'information au niveau fédéral. Les particularités du système gouvernemental et de la constitution fédérale de la Suisse rendent cependant la tâche d'une politique stratégique de l'information et de la communication en temps de crise difficile. Au niveau international, la Suisse pourrait apporter une contribution importante au niveau de l'éclaircissement des questions de droit international sur les opérations informationnelles. Elle pourrait aussi faire campagne pour un moratoire international sur le développement et la mise en œuvre des armes informatiques et sur la promotion de l'universalité d'accords visant à utiliser le cyberespace de manière pacifique.

- Editeur responsable: Daniel Möckli analysen@sipo.gess.ethz.ch
- Commande d'analyses et abonnement gratuit: www.ssn.ethz.ch