

## La Transformation en Suède : La Network-Based Defense mars 2005

L'Armée suédoise doit répondre à de nouveaux défis : elle doit gagner en précision (efficacité, faible coût, peu de dégâts collatéraux), et en régularité, surtout dans les combats rapprochés air-terre. En Irak et au Kosovo a été montrée la difficulté de cibler, depuis le ciel, des objectifs peu visibles, dispersés et mouvants. L'importance des médias est aussi un nouveau facteur à prendre en compte. Il faut enfin pouvoir lutter contre des ennemis disposant de nombreuses plates-formes et d'un faible niveau technologique. C'est le texte "*The New Defense – prepared for the next millenium*" publié en 1999 (cf. <http://www.rand.org/publications/TR/TR119/TR119.sum.pdf>), qui définit les nouvelles missions de l'Armée suédoise. Il s'agit de créer une armée moderne, flexible et polyvalente, sur la base du service national. Il faut être capable d'assurer la défense mais aussi de participer à des opérations internationales. Le programme suédois se donne 20 ans (2005-2025) pour parvenir à la possibilité de mener des guerres réseau-centrées. Le premier objectif est de mettre en place l'architecture de ce réseau, les infrastructures de communication qui le matérialisent, et un plan de gestion des capteurs destinés à alimenter ce réseau. Trois aspects se détachent de la réflexion suédoise : la question du coût, la question de l'accès au réseau et, plus précisément, la question du langage qui véhicule les informations.

C'est la FOI (Agence suédoise de recherche en défense) qui est chargée d'évaluer les coûts et bénéfices de l'évolution vers la NCW. Cela passe par une identification des fonctions qui doivent être servies par le réseau et une identification de ce qui est nécessaire à la mise en place de ce réseau (services, formation, technologie, financement). Le détail des fonctions opérationnelles et des infrastructures de réseau était, en juin 2004, remis à plus tard. Une première estimation sera effectuée pour identifier l'ensemble des opérations qu'il faudra mener, pour comprendre comment ces opérations seront menées et donc pour savoir quelle structure de réseau sera nécessaire. Les opérations qu'il y aura à mener ont été classées en quatre catégories : **Les opérations de combat** (défense aérienne, missiles) qui nécessiteront un commandement et un contrôle unifiés ; **les opérations en temps de paix**, qui demanderont une bonne maîtrise du ravitaillement et de la gestion du personnel ; **les opérations "inter agences"** où il faudra échanger les informations et les données avec les autres départements du gouvernement ; et **les opérations de coalition** (assistance humanitaire ou assistance aux autorités locales) qui demanderont de fortes capacités d'interopérabilité. Mais les coûts et les évolutions technologiques à prévoir sont importants, des priorités seront donc définies. Si la sécurité intérieure reste la priorité on se concentrera sur la communication au sein de l'Armée de l'Air et de la défense missiles-antimissile. Si on s'attache aux opérations internationales à l'étranger, ce sont les fonctions d'interface qui devront être travaillées. Pour l'instant, trois types d'opération ont reçu particulièrement d'attention dans le cadre d'une mise en réseau : la défense air-missile ; un commandement de combat unifié pour l'air la mer et la terre ; et une définition unifiée des cibles. On envisage aussi d'y intégrer les réponses aux catastrophes naturelles, aux dommages dus aux armes de destruction massive, à la gestion du ravitaillement, et à l'entraînement.

**Les méthodes de calcul des coûts.** Ici, l'expérience venue du secteur privé peut-être utile. **L'estimation Bottom-Up** : consiste à analyser en détail tout ce dont on a besoin : matériel, travail, infrastructure... ce qui permet en outre de bien avoir en tête les enjeux et l'utilité de chaque élément. **L'analogie** : permet de comparer avec d'autres systèmes. Une méthode utile et rapide quand on a un système évolué ou dérivé d'un autre, mais problématique quand les changements sont plus radicaux. **Prévisionnelle** : Il s'agit de disposer des bons paramètres permettant de calculer le coût supplémentaire pour telle évolution technologique ou telle nouvelle organisation. **Le calcul des coûts** : il faut estimer le coût de l'infrastructure, mais aussi celui de l'EBO elle-même, être capable de dire quels réseaux sont les plus rentables, et quelles opérations ont avantage à être mises en réseau, pour pouvoir éviter les surcoûts et afficher des priorités puisque tout ne peut être mis en réseau en même temps. Les coûts sont : celui du développement des concepts puis du système; celui de l'infrastructure – software, hardware - celui des tests. Il faut aussi considérer les coûts d'entretien et d'utilisation, puis d'évolution, ainsi que celui de l'estimation du coût d'un système presque entièrement nouveau. Il faut

ensuite pouvoir comparer le coût d'une opération réseau-centrée au coût de la même opération menée de manière classique. Que ce soit pour une question de coût ou tout simplement d'efficacité, la question d'un accès différencié au réseau se pose. Il faut distinguer les utilisateurs en fonction de leurs besoins en données, leurs tâches, les coûts, les questions de sécurité. Les catégories peuvent être distinguées en fonction du nombre de personnes qui doivent avoir accès aux informations, des nécessités de sécurisation du réseau, et du temps. Quatre catégories ont été définies. **L'interaction spécialisée** : chacun va chercher de son propre chef les informations en fonction de ses besoins. Il n'y a pas vraiment besoin de réseau. Cette catégorie représente l'accès traditionnel à l'information, c'est la catégorie témoin. A partir de là on définit les autres catégories en fonction de leurs : intensité, capacité, richesse, accessibilité, possibilité de contrôle, robustesse, sécurité, opportunité. **L'interaction quel que soit le lieu** : quand les opérations concernent un grand nombre de personnes (roulement, ravitaillement) il faut des données similaires accessibles au plus grand nombre. **L'interaction sécurisée** physiquement et électroniquement. Les demandes d'interaction se font sur le réseau, puis les échanges sont sécurisés. **L'interaction en temps réel** : il faut que peu de personnes aient accès à des informations critiques en temps réel. Et qu'elles puissent les distribuer à toutes les personnes nécessaires. Elle doit fonctionner même lors d'une défaillance du réseau. Ces prémisses posées, l'Armée suédoise a déjà développé la question de la création d'une image commune, utile et accessible à tous <http://www.sedris.org/stc/2004/pp/sweden/sld019.htm>. Il s'agit de transformer les informations géographiques grâce à une collaboration entre la Swedish Defense Research Agency (FOI), la Swedish Defense Material Administration (FMV) et la Armed Forces Support Organisation (GeoSe). La GeoSe fournit les informations géographiques qui doivent pouvoir être diffusées à toutes les armées, nationales et internationales alliées. L'enjeu est d'avoir des données à jour qui permettent d'aboutir à une image commune des champs de manœuvre. Cette image commune sera définie à partir de sondages déterminant les besoins en matière d'information, et écrite à l'aide d'un langage codé unique. Il faut des données plus nombreuses et à jour, qui doivent être utilisées pour des simulations et des exercices de coopérations internationales; d'où la nécessité de prendre en compte les normes internationales, et le besoin d'une formation adéquate. Mais le champ de bataille ne pourra être entièrement modélisé. Et ne pourra correspondre entièrement à ce qui est nécessaire. Les zones d'ombres apporteront des difficultés et des opportunités. La perception du champ de bataille dépendra toujours, en dernier lieu, du commandant, de sa culture, de sa formation, et de son expérience.