

Menace asymétrique et renseignement terrestre

Les B2 de la FAT ont un certain savoir-faire de l'élaboration du renseignement lors des opérations de coercition, fondé d'une part sur la formation spécialisée acquise et les méthodes qu'elle enseigne, d'autre part sur la pratique des exercices au CEPC (AURIGE, GUIBERT). Les bases nécessaires pour le **traitement des menaces asymétriques** lors des autres types d'action (stabilisation, assistance), ont certes fait l'objet d'une réflexion importante, mais sont moins établies et demandent des actions complémentaires en matière d'outils et de méthodes.

Après une réflexion sur les caractéristiques de la menace asymétrique, cet article proposera des voies à explorer en s'appuyant sur l'expérience déjà acquise par l'EMF 4 au cours de plusieurs engagements en opération extérieure, permettant d'en déduire des actions à mener au profit de la fonction renseignement afin de développer sa compréhension de situation.

PAR LE LIEUTENANT-COLONEL DIDIER SIMON (EMF 4)

Caractéristiques de la menace asymétrique

Sans se lancer dans une présentation exhaustive du sujet que l'on peut trouver dans des auteurs universitaires, cette menace présente, pour un B2, les **principales caractéristiques** suivantes :

- Tout d'abord, il ne s'agit pas d'un combat cantonné dans le niveau tactique avec des acteurs bien identifiés en nombre limité et aux modes d'action relativement connus, mais d'**une confrontation beaucoup plus globale** dépassant les champs strictement militaires de confrontation pour englober l'idéologique, le politico-ethnique, le culturel et le religieux, comme dans les guerres de libération nationale, les actions de guérillas, et les autres conflits inter - ou surtout intraétatiques qui dégénèrent en action de violence collective.

La bonne perception de cet environnement est indispensable, d'une part pour comprendre le milieu dans lequel intervient la FOT et avec lequel elle devra interagir, qu'elle le veuille ou non, d'autre part parce que ce milieu est inévitablement - de manière certes très variable selon les cas - le "sanctuaire", le vivier et la base arrière des acteurs de ces menaces.

- Ensuite, ce qui est le propre de l'asymétrie, l'adversaire de nos forces en opération refusant le "combat en ligne" pour lequel il serait déclassé technologiquement, va chercher à **agir sur nos vulnérabilités**,

en compensant par la surprise son infériorité numérique : la concentration des efforts reste en effet un principe de la guerre, même asymétrique. Il ne peut donc agir fort ... en étant faible, que là où nous sommes nous-mêmes très faibles, d'où une **importance capitale de la surprise**, le parangon des modes d'action correspondant étant l'attentat terroriste. L'attaquant s'efforcera de toujours disposer de l'initiative en choisissant le lieu et l'heure, alors qu'à l'inverse la défense (l'auteur considère qu'en maîtrise de la violence les forces se retrouvent de facto en posture défensive), du fait des contraintes légales et des règles d'engagement, ne peut engager des moyens identiques.

- Enfin, ce qui rejoint la préoccupation évoquée en premier, l'adversaire ne compte **pas uniquement sur l'aspect purement militaire** de son action, mais compte beaucoup sur des multiplicateurs d'efficacité, même s'il ne pratique pas ce vocable, en l'occurrence l'aide des populations, ou simplement la réaction des populations et l'opinion internationale. Elle se traduira en général par une **stratégie indirecte** où la capacité de nuisance s'appuie en partie sur les leviers de pouvoir que sont des organisations "patriotiques", d'anciens combattants, des mouvements communautaires, ethniques, de jeunesse, de femmes, etc. eux-mêmes au centre d'une "nébuleuse" qui tend souvent à prendre un caractère mafieux, en réponse à des besoins de financement.

Les **principaux procédés couramment mis en œuvre** par ces acteurs sont :

- **Les actions de surveillance** qui consistent à tester localement la capacité, les délais de réaction et d'implication de la force engagée dans la mission, ainsi que les points d'application de ses mesures de sûreté.
- **Les actions de déception**, qui consistent à maintenir les autorités et les états-majors des forces sous pression afin de mieux accaparer ou focaliser et/ou détourner leur attention, pour favoriser l'atteinte d'un objectif.
- On trouve, par ailleurs, **des actions qui visent à discréditer**, délégitimer la force en tentant de la pousser à la faute par une réaction disproportionnée ou au contraire par une absence "coupable" de réaction.
- Finalement, **celles dont l'objectif détecté est de développer une ambiance générale de terreur** afin de mettre en place les conditions d'une paralysie générale et communicative destinée à inhiber les décideurs (événements d'Abidjan de novembre 2004 contre les expatriés français).

Les actions de déception peuvent s'accompagner de **manœuvres d'intoxication**, et, à l'expérience des théâtres balkaniques, la multiplication des capteurs et la rareté des sources ont même parfois mené nos forces à l'auto-intoxication.

Les outils du renseignement

Sans s'attarder sur les évolutions en cours ou à mener au titre des capacités de recherche, traitées par d'autres auteurs, il s'agit maintenant de **voir quels sont les moyens et méthodes d'analyse disponibles pour prendre en compte cette menace**.

Le **premier travail mené par un B2 dans ce cadre est celui de la préparation renseignement de l'environnement opérationnel (PREO)**, qui doit être



déroulé dans les moindres détails, en particulier dans l'étude de l'environnement physique, humain (gouvernement, associations, forces de sécurité), sans négliger la géographie humaine : composition ethnique, répartition géographique et problèmes (récurrents ou factuels), biographie des leaders, etc.

Cette démarche analytique ne doit pas être considérée comme un produit fini, mais doit être relancée par :

- **Une analyse culturelle/ethno-religieuse/politique/économique**, constituant le fond documentaire d'une base de données⁴, élément essentiel de référence à disposition du théâtre. Pour que l'on puisse parler de "référence", il doit s'agir d'un **outil commun à tous les niveaux** (de la DRM au GTIA) et remis à jour perpétuellement, d'un emploi simple, par exemple fonctionnant à l'aide de mots-clés ou de faits.

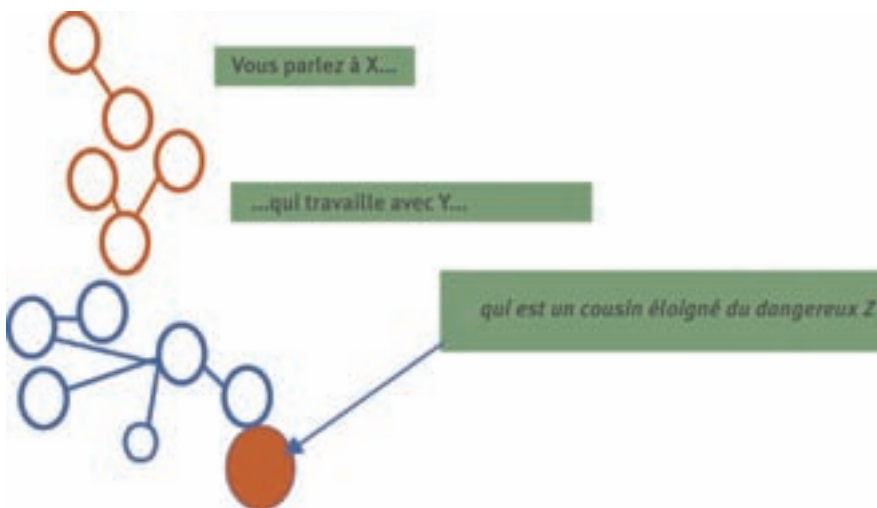
Si tout G2 en opération dispose actuellement d'un fonds documentaire, dont la **transmission d'un mandat à l'autre** est toujours source de difficultés, justement par manque de support, l'objectif formalisé ci-dessus reste aujourd'hui de l'ordre de l'idéal, cette notion n'ayant pas encore fait l'objet de réalisation ni même d'analyse sur le fonds au niveau national, tant en matière de contenu que d'application informatique susceptible d'en représenter le support. Des expériences ont néanmoins été faites dans le cadre de SFOR et KFOR (base JOIS employée par l'OTAN). L'application IDELIANCE, déployée en Côte d'Ivoire et présentée par ailleurs s'en rapproche.

Cette base sert, notamment, à déterminer les structures sociales prévalant en matière d'autorité, d'allégeance (gouvernementale, politique, clanique, tribale et religieuse) dans les lieux où la force est déployée et ce, pour produire un "story board" politico-culturel.

- **Des analyses systémiques du milieu**. Ces analyses sont nécessaires pour la compréhension des organisations humaines, a fortiori les organisations clandestines. Les méthodes correspondantes sont encore largement expérimentales et de toute façon méconnues dans le milieu militaire, même si certaines commencent à avoir une certaine application opérationnelle dans le sein des "services" et de l'institution judiciaire. Le logiciel ANACRYM, qui permet de faire de l'analyse relationnelle et qui est mis en oeuvre par la gendarmerie pour étudier les réseaux criminels en métropole, en est une illustration.

A titre d'illustration, la figure ci-contre offre **une représentation de groupes humains organisés en "cellules"** (au sens des théoriciens de la guerre révolutionnaire) indépendantes, avec un seul point de convergence qui est le but commun (phobie ethnique, politique, religieuse etc.) mais sans linéarité ni contiguïté, dans l'exemple de la guerre sans front :

Une telle organisation n'empêche une analyse des liens dans les actions, communications, symboles etc. :



Cette analyse peut, par ailleurs, faire apparaître une "nébuleuse" qui n'avait pas été identifiée auparavant, la recherche des "signaux faibles" étant très importante dans l'analyse de ces menaces.

• **Des "analyses des occurrences"**. Les adversaires suivent généralement une phase de montée en puissance qu'il s'agira de détecter au plus tôt, puis survient une séquence d'actions qu'il s'agit d'analyser finement² et ce, pour ne plus en être en réaction mais **prédictif**. Par ailleurs, il faut déterminer autant d'indicateurs possibles (affiches, graffitis, manifestations, discours enflammés, articles de presse partisans et inflammatoires) associés à un chronogramme des éléments prévisibles (élections, fêtes religieuses, etc.) qui puissent aider à définir les occurrences des actions ou pour le moins **une tendance** générale.

Le problème devient ardu avec les théâtres "dormants" comme le KOSOVO où les actions spectaculaires et analysables sont extrêmement rares (attentat du pont au nord de MITROVICA en avril 2003 et émeutes anti-serbes de mars 2004 qui confirment la tendance bien connue de l'offensive de printemps de l'ex - UCK et de ses avatars). L'exercice devient particulièrement complexe quand des phases d'action s'inscrivent dans l'irrationnel et l'imprévisible (bombardement des troupes françaises par les avions des FANCI).

Par ailleurs, la **capacité du B2** à mener des analyses d'événements, et, ce que l'on attend surtout de lui, à anticiper des agressions ou des situations de tension dépendra de sa **compréhension en profondeur du milieu** et de sa maîtrise de ses "codes de communications", qu'ils soient ouverts ou clandestins. Il faut donc développer une expertise en analyse de

communication-linguistique avec des spécialistes des relations avec les médias, en mesure de décrypter les messages subliminaux ainsi que les opérations psychologiques conduites par l'adversaire qui manipulent les médias, expertise peu disponible dans les armées, sauf peut-être chez certains ESR ayant le bagage professionnel civil correspondant.

Enfin, on ne peut plus faire l'impasse sur une expertise en matière d'analyse légale et scientifique (en terme de résolution de crime) qui nécessite l'appui de la gendarmerie, pour développer des procédures d'enquête servant à analyser, comprendre et exploiter les procédés ou techniques et en cela évaluer les vulnérabilités adverses potentielles. La

problématique des IED³ que les forces terrestres subissent en Afghanistan illustre particulièrement ce propos.

Face à la menace présentée dans la première partie de cet article, les points qui viennent d'être évoqués montrent bien que, tel le M. JOURDAIN de Molière qui "faisait de la prose sans le savoir" - et donc, de manière imparfaite -, **l'officier du G2 analyse la menace asymétrique de manière qui reste "artisanale"**, même s'il a des idées sur des méthodes et des outils qui lui permettraient de professionnaliser sa prise en compte de cette menace pour anticiper son action et apporter au chef interarmes la liberté d'action dont il a besoin.

Il s'agit maintenant de **proposer des voies pour développer les capacités d'exploitation** des G2 d'une force terrestre.

Les efforts à consentir au profit du renseignement

Cet article n'a pas vocation à développer les questions de la "recherche", mais il apparaît naturellement, d'après les thèmes d'intérêt présentés (qui rejoignent ce que l'on appelle les **PIR - Priority Intelligence Requirements** - besoins prioritaires en renseignement du chef interarmes), ce qui est confirmé par de nombreux RETEX, que le renseignement sur le milieu humain, notamment les acteurs de violence, actuels ou potentiels, affichés et a fortiori clandestins, ne peut être acquis que par des capteurs humains, ce qui demande un **investissement important de l'armée de terre dans le domaine du ROHUM**.

Il faut également développer et coordonner une **expertise contre-ingérence à large échelle**, malgré les difficultés de pénétration d'un milieu humain généralement fermé et hostile et en dépit des contraintes d'un cadre légal et juridique qui ne permet pas, aujourd'hui, une posture offensive des moyens ROHUM pour conduire des actions intrusives de recherche.

Cette capacité de **recherche** étant renforcée, il faut ensuite **disposer d'outils d'exploitation** permettant au G2 de remplir sa mission de manière professionnelle.

Le premier besoin est celui d'une **base de connaissances** au profit du renseignement - mais pouvant être, au moins partiellement, accessible à d'autres utilisateurs selon le principe de la mise à disposition du renseignement validé. Cette base de connaissances doit correspondre idéalement à un **modèle stable, disponible en opérations comme en métropole, interopérable** avec la base de renseignements validés de la DRM, ou au minimum l'application de GED dont dispose la FRENIC des théâtres. La disponibilité d'un tel outil représentera un progrès considérable dans l'efficacité d'un G2 dans les opérations de stabilisation. Il constituerait également un outil puissant de MCO de ces G2 avant projection. Il restera ensuite à veiller à ce qu'il soit alimenté avec rigueur, ce qui est surtout une affaire de discipline intellectuelle, les outils puissants étant loin d'être toujours des outils simples d'accès !

Le second besoin est celui d'**applications logicielles d'aide à l'analyse des menaces**, ou au minimum de méthodes de raisonnement. L'exemple d'ANACRYM a été évoqué. Des outils existent et sont en service dans certains organismes, d'autres seraient à développer, mais il y a lieu de dépasser le "travail à la main" qui reste encore le lot commun.

Ces deux capacités ne seront réellement valorisées que si elles sont accessibles en réseau, ce qui conduit à un **besoin de liens à haut débit** pour les activités

renseignement interarmées ou tactiques, avec la possibilité d'un appui délocalisé "**reach-back**" (hors théâtre éventuellement) de la part d'experts pointus par domaine et d'analystes renseignement **pour l'obtention d'autres perspectives** (renseignement des pays voisins, analystes en économie politique).

Ces capacités étant disponibles, on pourra alors identifier puis isoler les cellules adverses en les coupant du reste de la société considérée, puis essayer de détourner leur attention pour les mettre au minimum en posture défensive et finalement établir leurs vulnérabilités (tensions, rivalités etc.), travail du RENS permettant l'engagement opérationnel.

Ce type d'actions ne se conçoit cependant que **sur le long terme**, ce qui demande d'**établir une "mémoire institutionnelle"** et de stabiliser la fonction renseignement, d'où la nécessité pour les acteurs de s'inscrire dans la durée. Pour la fonction renseignement, les mandats devraient être tous de 6 mois ou 1 an pour tirer un maximum de l'expérience et de la compréhension acquises.

Enfin, en amont de la mise en œuvre de ces savoir-faire, il y a leur définition et la conduite des **actions de formation correspondantes**. Sans tomber dans l'hyper-spécialisation évoquée dans certains documents, comme le recours à des anthropologues ou des sociologues, car il y a le risque pour les S2 et G2 de rajouter du brouillard au "brouillard de la guerre", un approfondissement de la formation au CEERAT pour une bonne prise en compte de ces menaces est souhaitable.

1 Idéalement d'une "base de connaissances" mais il faut partir de ce que permet l'état de l'art et de nos connaissances initiales.

2 Un tableur permet déjà un bon stockage d'informations traitées ainsi qu'une visualisation spatio-temporelle ou par type d'actions.

3 IED : Improvised Explosives Devices, engins explosifs improvisés.

L'armée de terre est exposée, depuis plusieurs années déjà, à des menaces asymétriques sur les théâtres où elle est déployée, même si elle n'a, par chance, pas eu l'occasion de confrontations aussi violentes que celle que rencontrent nos alliés en Irak. Un effort significatif a été fait par les G2 pour prendre en compte ces menaces, en développer l'analyse tant pour la sauvegarde de nos forces que pour permettre leur neutralisation.

Il s'agit maintenant, surtout à la lumière du déchaînement de la violence que l'on peut voir sur certains théâtres et qui est susceptible de faire tâche d'huile, de **professionnaliser nos méthodes d'exploitation**. Il faut, en quelque sorte, répondre de façon asymétrique à une asymétrie, non pas en épousant les méthodes ou techniques de l'adversaire mais bien en s'appropriant sa culture, ses structures mentales pour penser comme lui mais aussi plus vite que lui. Il faut aussi **faire progresser nos méthodes d'analyse**.

Ce défi est à la portée de l'armée de terre et les EMF peuvent mettre leur expertise à disposition de ceux qui le prendront en compte.