

# Continuité de la menace

## Du territoire national aux théâtres d'opérations

Les forces terrestres font, en opération extérieure, l'objet de **menaces de la part d'organisations ou d'individus qui cherchent à leur porter atteinte par d'autres voies que la confrontation militaire**. Ces menaces sont qualifiées d'ingérences. Ces ingérences ou tentatives d'ingérences, déjà existantes en période normale, sont renforcées en opérations, que ce soit sur le théâtre en cause, ou même en dehors du théâtre, pouvant même se prolonger par des actions hostiles en métropole, notamment de la part d'organismes ou de groupes ayant une implantation ou une capacité d'action multinationale.

Cet article proposera un bilan de ces menaces puis quelques réflexions sur l'évolution de la situation actuelle pour conclure par quelques recommandations.

---

PAR LE GÉNÉRAL DE DIVISION DENIS SERPOLLET, DIRECTEUR DE LA PROTECTION ET DE LA SÉCURITÉ DE DÉFENSE

---

### Quelle menace ?

**Les principales ingérences auxquelles une force terrestre doit faire face** sont le terrorisme, l'espionnage, le sabotage, la subversion et le crime organisé (**TESSCO**).

- Le **terrorisme** consiste en l'utilisation illégale ou la menace d'utilisation de la force ou de la violence pour contraindre ou intimider les gouvernements et les sociétés afin d'atteindre des objectifs politiques, ethniques, religieux ou idéologiques. Il est destiné à frapper les esprits, à les soumettre et à imposer une volonté minoritaire par l'horreur qu'il provoque à dessein.

- L'**espionnage** est la méthode secrète utilisée par une puissance étrangère ou d'autres groupes d'intérêts pour acquérir les informations auxquelles ils n'ont pas accès.

- Le **sabotage** consiste en la destruction ou la neutralisation de matériels essentiels aux opérations des forces amies en vue de perturber leur manœuvre.

- La **subversion** est définie comme une action conçue pour affaiblir la force militaire, économique ou politique d'une nation en minant le moral, la fidélité ou le sérieux de ses citoyens. En opérations, le but recherché est de démonstrer la force par des opéra-

tions conçues pour neutraliser ou amoindrir son efficacité au combat de la force. Une attaque subversive est difficile à détecter et à contrer.

- Le **crime organisé** peut être décrit comme une action des organismes à caractère criminel ayant pour objectif de gagner illégalement une forme de puissance par influence ou argent, et en faisant abstraction des lois démocratiques du pays dans lequel ils opèrent. En opérations, les divers trafics (drogue, prostitution, matériels ou produits contrefaits ou de contrebande, armes) sollicitent directement les membres de la force et peuvent en affaiblir le potentiel, voire porter atteinte à sa crédibilité.

La menace est principalement constituée par l'action des services de renseignement adverses, des forces spéciales de l'adversaire ou des belligérants, des organismes, groupes ou individus terroristes, les organismes, groupes ou individus subversifs ou des organisations et groupes criminels.

Si, jusqu'à la disparition de l'ex-URSS, cette menace était principalement représentée par l'action des "services" de l'URSS, ainsi que celles de ses alliés officiels (pays de l'Est, par exemple) ou objectifs, qu'ils soient financés par elle, simples compagnons de route voire groupes ou individus alliés objectifs (diverses organisations terroristes du Moyen-Orient, certaines organisations pacifistes ou anti-nucléaires, etc.), cette menace s'est fortement diversifiée. La déliquescence de l'ex-URSS

et le développement de la grande criminalité qu'elle a entraîné dans cette zone d'une part, le développement du fondamentalisme musulman et les groupes terroristes fanatisés qui s'en réclament d'autre part, ont complètement diversifié cette menace et l'ont rendue difficile à comprendre et maîtriser.

### Une menace permanente sur les théâtres

Cette menace n'est plus anecdotique ni même secondaire pour nos forces en opération. On peut la préciser en reprenant la présentation conventionnelle des opérations issue de la notion de "continuum des opérations", développée par l'OTAN<sup>1</sup> et complétée par la vision française exprimée dans le concept de stabilisation.

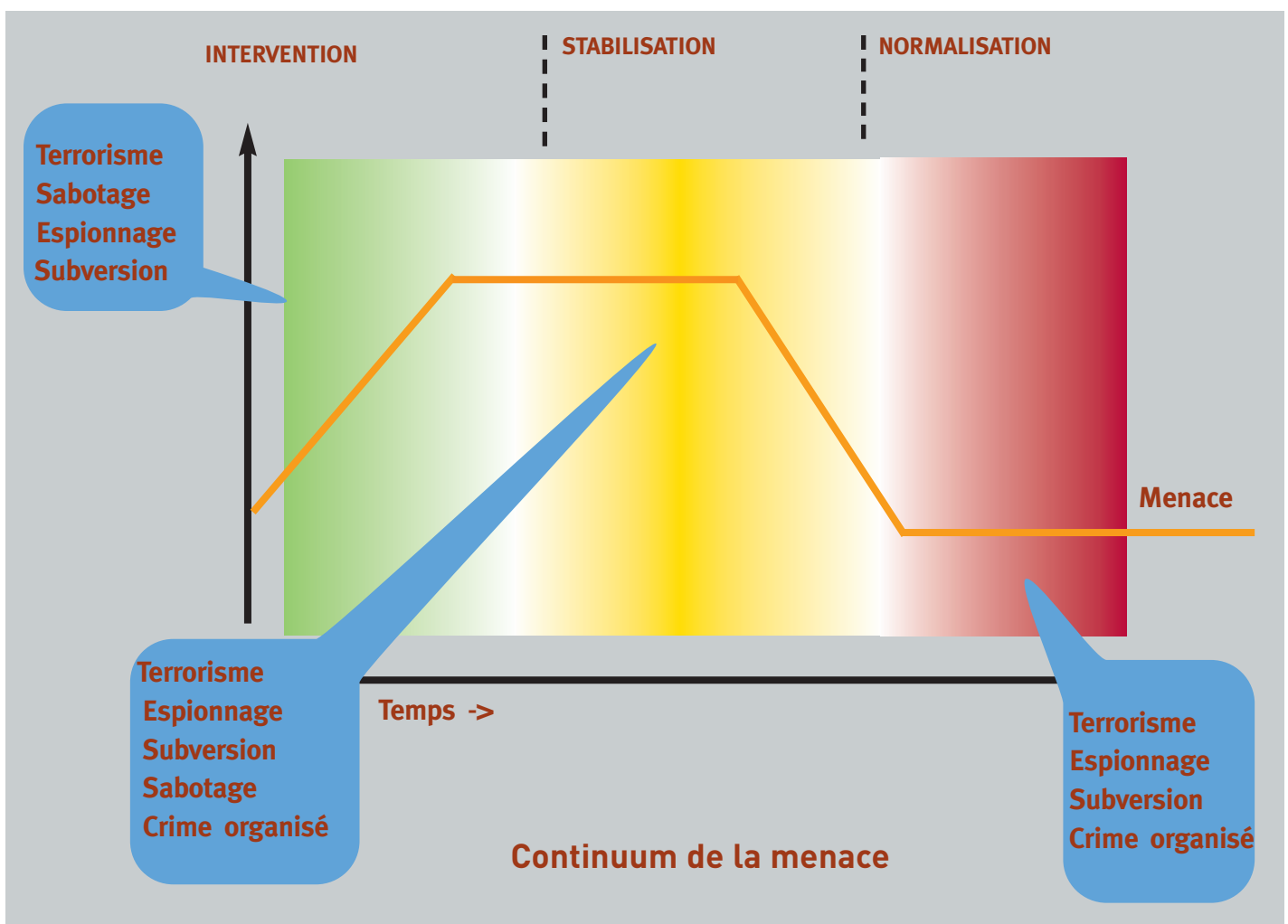
A la différence d'une guerre classique comportant une phase de combats intenses suivie de la signature d'une paix et de l'arrêt complet de la violence, les opérations actuelles peuvent se décomposer en trois phases : intervention, stabilisation et normalisation. Dans ce contexte, **la menace TESSCO est toujours présente mais à des degrés divers, en fonction des phases de l'opération.**

Le schéma ci-dessous représente d'une manière théorique, la caractérisation de la menace :

Quelle que soit la phase de l'opération, **la menace terroriste est la plus flagrante** et aura une part importante dans les opérations à venir. On peut cependant penser que les forces sont en position plus

favorables pour la combattre lors de la phase d'intervention dans les actions de coercition, les règles d'engagement du moment et la posture de la force lui donnant une meilleure capacité défensive. La menace est en revanche **la plus grande dans la phase de stabilisation**, comme l'Irak en offre un exemple tragique aujourd'hui : la force a dû se déployer et s'imbriquer au moins partiellement avec les populations locales, les règles d'engagement se sont adoucies, l'acceptation de la force par les acteurs locaux est loin d'être totale et des groupes armés subsistent.

Il convient toutefois de **ne pas négliger les autres et plus particulièrement l'espionnage** systématiquement pratiqué par les services de renseignements locaux et facilité par le recours aux



ressortissants du pays employés par la force. Cette menace est à la base de toutes les ingérences, car aucune d'entre elles ne peut être menée contre une force sans l'acquisition de l'information. Une action de terrorisme ou de sabotage est, en effet, toujours précédée d'une collecte d'informations nécessaires à la désignation de l'objectif et au choix du mode d'action, l'action terroriste étant, en fait, une action ciblée de manière précise pour agir sur nos vulnérabilités, beaucoup plus psychologiques que réellement militaires.

Une **action subversive**, également, ne peut être efficace que si l'adversaire connaît l'état du moral des membres de la force et leurs points faibles. Elle se traduira donc par des actions de recherche adverses sur notre organisation, nos motivations, la compréhension des motivations réelles de la force. Elle cherchera également à identifier comment discréditer les chefs de la force ou leurs leaders d'opinions, ainsi qu'à détecter des membres de la force qu'elle pourrait convertir/retourner et utiliser comme relais.

Les organisations criminelles ne peuvent développer leurs **trafics** au sein d'une force que si elles en connaissent les rouages. Elles aussi rechercheront les "maillons faibles" pour les corrompre et les utiliser à leur profit.

Force est de constater aussi que les différents acteurs n'agissent pas exclusivement dans leur domaine préférentiel de TESSCO : sans utiliser sans doute ce vocabulaire, ils ont compris et employé avant les armées les principes de "polyvalence", "info-valorisation", voire "synergie des effets" !

Ainsi des **organisations terroristes** trouvent leur financement grâce à des pratiques criminelles (trafics de drogue, attaques de banque,...) ; des organisations criminelles n'hésitent pas à commettre des actes terroristes pour affaiblir les Etats (par exemple : les cartels en Colombie). Par le passé, des services de renseignement ont utilisé des mouvements terroristes pour contrer leurs adversaires (i.e. l'attentat contre le pape imputé aux services de renseignements soviétiques). En Irak, il est difficile de faire la part du criminel ou du terrorisme dans les prises d'otages.

Une difficulté importante rencontrée par une force est que les services, organisations et individus pratiquant le TESSCO bénéficient du **soutien actif ou, a minima, de la neutralité de tout ou partie de la population locale**, qu'il s'agisse d'une opération nationale comme en Côte d'Ivoire ou multinationale comme en Afghanistan. Ils évoluent dans leur milieu et en sont d'autant plus difficiles à détecter et à neutraliser.

### Une menace sans limite géographique

Une autre caractéristique des ingérences modernes tient au fait qu'elles ne se limitent pas au cadre espace-temps de l'opération. Le développement des moyens de communication, physiques ou de télécommunications, le rôle considérable d'influence joué par les médias, ont fait éclater les cadres géographiques et étatiques, sinon pour l'action de nos forces contraintes par les règles de droit et les traités, mais en tout cas par la menace étudiée qui s'affranchit de ces limites sans difficulté.

**Les activités liées aux ingérences peuvent ainsi être déclenchées à l'extérieur de la zone d'opération**, voire avant son déclenchement. Ces ingérences préalables peuvent participer à la dissuasion adverse, et contribuent à son propre renseignement avant les actions d'importance au sein du jeu politico-militaire qui précède et accompagne l'engagement militaire. Il n'est pas concevable d'imaginer désormais d'opérations militaires qui n'aient pas de répercussions sur le territoire national ou partout dans le monde où la France a des intérêts. Les attentats du 6 octobre 2002 contre le pétrolier français "Limburg", dans les eaux yéménites, et du 8 mai 2004 contre le personnel de la direction des constructions navales à Karachi en sont l'illustration. La France a été visée parce qu'elle participe activement aux opérations en Afghanistan. Comme sur les théâtres d'opération, la menace terroriste est la plus flagrante mais il ne faut pas non plus négliger les autres menaces.

Ainsi lors des opérations aériennes contre la Serbie en 1999, un officier français, en poste à l'OTAN, a fourni aux Serbes des informations sur les cibles. Certains personnels de la défense font l'objet d'approches de la part de services de renseignement et comme toujours dans ce type d'affaire, pour une connue, combien restent cachées ?

### La menace la plus insidieuse reste la subversion.

Elle est aussi la plus difficile à combattre, dans la mesure où elle se traduit rarement par des actes susceptibles de qualifications juridiques de crimes ou délits. Sur le territoire national, elle s'adresse à l'opinion publique. Dans nos sociétés hyper-médiatisées, la moindre informa-

tion bénéficie d'une caisse de résonance phénoménale amplifiée par Internet. La diffusion des images de la prison d'Abou Grahib illustre bien ce propos. Les organisations ou individus subversifs bénéficient, dans leur lutte, de **l'aide volontaire ou non d'agents d'influence**, au premier rang desquels les chaînes de télévision. Au Vietnam, l'opinion américaine a basculé contre la guerre en grande partie en raison des reportages qui montraient en quasi direct les réalités du conflit. Ce type d'informations correctement manipulées par des techniciens de la désinformation aura des effets non dépourvus de conséquences sur les théâtres.

Pour pouvoir perpétrer leurs actes loin de leurs bases, les services et organisations doivent pouvoir bénéficier de **soutien dans les pays où ils agissent**. Une des caractéristiques des sociétés démocratiques occidentales, dont la France, est l'extrême diversité de leur population, notamment ethnique par la présence de communautés plus ou moins importantes originaires des pays de la zone d'opération avec, comme corollaire, une grande diversité religieuse ou idéologique. C'est au sein de ces communautés que se recrutent des activistes et que se développent les réseaux "dormants" ou de soutien.

### Contre la menace

Comme le dit le sage africain, "l'étranger ne voit que ce qu'il connaît". La connaissance de la menace est la première étape de la contre-ingérence. Les deux autres sont sa détection et sa neutralisation.

**Détecter la menace** consiste à recueillir le renseignement de sécurité et à collecter les faits et indices, à les exploiter dans le but de fournir au commandant de la force une appréciation de la menace.

**Neutraliser la menace** consiste tout d'abord pour le commandement à prendre les mesures qui doivent permettre la réalisation de l'état de sécurité. C'est-à-dire obtenir une protection satisfaisante des informations, du matériel et des installations sensibles contre le terrorisme, l'espionnage et le sabotage et par celle du personnel contre la subversion et le crime organisé.

La contre-ingérence en opération est une des missions de la direction de la protection et de la sécurité de la défense. Cependant, l'action à mener ne se limite pas à celle des spé-

cialistes, à ceux que l'on pourrait considérer comme "les professionnels de la méfiance". En matière d'organisation, la **coordination des actions de contre-ingérence** dans une unité multinationale projetée a vocation à s'effectuer au sein de la structure de G2X, en mettant à profit le concept développé par l'AJP 2.1, doctrine approuvée par la France et qu'il faudrait traduire dans les faits, en identifiant les structures et en rédigeant les procédures correspondantes. Nos organisations seront alors en cohérence avec celles de nos alliés avec lesquels nous sommes amenés à nous engager de plus fréquemment. La DPSD possède des cadres formés qui ont vocation à armer les cellules correspondantes de ce G2X. Lorsque des cas particuliers sont identifiés concernant des nationaux, la chaîne multina-

tionale les passe en compte à la chaîne nationale qui entreprend alors les mesures nécessaires. Sur le théâtre, cette chaîne est représentée par le détachement PSD déployé avec la force. Il apporte son concours aux différents niveaux de commandement des élé-

ments nationaux pour l'exercice de leurs responsabilités en matière de sécurité et en premier lieu au COMANFOR en opération nationale ou au REPFRANCE en opération multinationale.

1 AJP 3.2, Chap. 1.6

**Le comportement de tout un chacun est cependant être la première ligne de défense face à la menace adverse :** respect des règles de sécurité, pas d'angélisme même vis-à-vis de locaux d'apparence angélique, ne pas hésiter à se poser la question de l'intention adverse et ses modes d'action possibles, etc. Si le renseignement est en partie "l'affaire de tous" au titre de la culture à posséder et de la contribution de tout personnel au recueil des informations, **la contre-ingérence ne peut pas reposer sur la seule compétence d'un nombre restreint de spécialistes.**

Elle doit être intégrée dans une culture de discrétion, de sécurité et de vigilance.

