Études de l'Ifri
Focus stratégique 71

LES MUTATIONS DU RENSEIGNEMENT MILITAIRE

Dissiper le brouillard de la guerre ?

Joseph HENROTIN

Janvier 2017

ifri Laboratoire de Recherche sur la Défense

L'Ifri est, en France, le principal centre indépendant de recherche, d'information et de débat sur les grandes questions internationales. Créé en 1979 par Thierry de Montbrial, l'Ifri est une association reconnue d'utilité publique (loi de 1901). Il n'est soumis à aucune tutelle administrative, définit librement ses activités et publie régulièrement ses travaux.

L'Ifri associe, au travers de ses études et de ses débats, dans une démarche interdisciplinaire, décideurs politiques et experts à l'échelle internationale.

Avec son antenne de Bruxelles (Ifri-Bruxelles), l'Ifri s'impose comme un des rares *think tanks* français à se positionner au cœur même du débat européen.

ISBN : 978-2-36567-672-4

Comment citer cette publication :

Joseph Henrotin, « Les mutations du renseignement militaire. Dissiper le brouillard de la guerre ? », *Focus Stratégique*, n° 71, Ifri, janvier 2017.

Ifri

27 rue de la Procession 75740 Paris Cedex 15 – FRANCE

Tél. : +33 (0)1 40 61 60 00 – Fax : +33 (0)1 40 61 60 60

E-mail : accueil@ifri.org

Ifri-Bruxelles

Rue Marie-Thérèse, 21 1000 – Bruxelles – BELGIQUE

Tél. : +32 (0)2 238 51 10 – Fax : +32 (0)2 238 51 15

E-mail : bruxelles@ifri.org

Site internet : Ifri.org

Focus stratégique

Les questions de sécurité exigent une approche intégrée, qui prenne en compte à la fois les aspects régionaux et globaux, les dynamiques technologiques et militaires mais aussi médiatiques et humaines, ou encore la dimension nouvelle acquise par le terrorisme ou la stabilisation post-conflit. Dans cette perspective, le Centre des études de sécurité se propose, par la collection ***Focus stratégique***, d'éclairer par des perspectives renouvelées toutes les problématiques actuelles de la sécurité.

Associant les chercheurs du centre des études de sécurité de l'Ifri et des experts extérieurs, ***Focus stratégique*** fait alterner travaux généralistes et analyses plus spécialisées, réalisées en particulier par l'équipe du Laboratoire de Recherche sur la Défense (LRD).

Auteur

Joseph Henrotin est docteur en science politique, chargé de recherche au Centre d'analyse et de prévision des risques internationaux (CAPRI) et à l'Institut de stratégie comparée (ISC). Auteur ou directeur d'une dizaine d'ouvrages et de plus de 600 articles, il enseigne dans les écoles de guerre de Bruxelles et Yaoundé, intervient dans plusieurs cycles d'études civils et militaires et est rédacteur en chef de *Défense & Sécurité internationale*. Il vient de publier *L'art de la guerre à l'âge des réseaux* (ISTE, 2017).

Comité de rédaction

Résumé

Le renseignement militaire a connu des évolutions majeures du fait de la technologie mais aussi des changements dans le caractère des opérations. Au cœur du projet de « révolution dans les affaires militaires », il devait contribuer à dissiper définitivement le brouillard de la guerre et à rendre le champ de bataille transparent. Les deux dernières décennies d'opérations en ont pourtant démontré qu'il en allait autrement : face à des adversaires complexes étroitement mêlés à leur terrain, les armées ont dû évoluer vers la notion de « renseignement d'intérêt militaire », élargissant ainsi le spectre de leur mission. En France, cette transformation a soulevé de nouvelles questions quant à l'organisation mais aussi aux moyens attribués au renseignement dans les armées et au sein de l'appareil de défense. Face aux nombreux défis technologiques, liés autant à la collecte qu'à l'analyse, l'avenir du renseignement militaire dépend plus que jamais des ressources, humaines et financières, que les décideurs voudront bien lui attribuer.

Abstract

Military intelligence has evolved significantly as a result of advanced technology and the changing character of war. In the 1990s, military intelligence was at the core of the "revolution in military affairs", carrying the hope that it would help dissipate the fog of war and increase transparency on the battlefield. However, because of the last two decades of military operations, this transformation has proved challenging. Confronted with increasingly complex opponents, Western armed forces have had to adopt the concept of "military interest intelligence", which widens the scope of its mission. In France, this transformation has borne many questions regarding intelligence organization and capabilities at both the service and joint levels. Given current technological challenges, both for collection and analysis, the future of military intelligence depends, more than ever, upon the amount of human and financial resources political and military leaders choose to allocate to this domain.

Sommaire

Introduction

En devenant une fonction stratégique à part entière dans les *Livres blancs sur la Défense et la Sécurité nationale* de 2008 et 2013, la « connaissance et l'anticipation » ont attiré l'attention sur le renseignement[1]. Mais de quel renseignement s'agit-il ? Longtemps considéré comme la « face cachée » des relations internationales, le renseignement est le plus souvent célébré dans sa dimension politico-stratégique avec, en ligne de mire, les « grandes agences » que sont la CIA, la NSA, le MI6 ou encore la DGSE. Également bien connus du grand public pour leurs « chasses aux espions » et, plus récemment, pour leur lutte contre le terrorisme, les organes de sécurité intérieure (FBI, FSB, MI5, DGSI, etc.) structurent quant à eux le champ du renseignement intérieur. Enfin, la période de l'après-guerre froide a vu émerger le dynamique secteur du renseignement économique – jadis connu sous le terme d'« espionnage industriel » – en introduisant de nombreux acteurs privés ou parapublics dans ce club jusqu'alors très fermé.

Dans ce paysage hétéroclite, on peine parfois à comprendre où se situe la spécificité du renseignement d'intérêt militaire. Dans le cadre de cette publication, nous l'entendons comme le processus de collecte, d'analyse, de dissémination et d'exploitation de l'information d'origine et d'intérêt militaire, plus particulièrement dans le contexte de la conduite des opérations. Cette seule définition renvoie, en réalité, à un objet dont le champ d'application est particulièrement vaste. S'il s'agit évidemment de se renseigner sur les capacités et les intentions d'adversaires avérés ou potentiels, il implique aussi de maintenir une veille – stratégique, technologique, doctrinale, etc. – ou encore de renseigner la situation dans un théâtre d'opérations en particulier. Le renseignement d'intérêt militaire recouvre aussi bien des aspects militaires *stricto sensu* (ordres de bataille, capacités) qu'une foule de données utiles à la planification et l'exécution des opérations : détermination et caractérisation des acteurs politiques, médiatiques, civils, spécificités de l'environnement sociopolitique et ambiance générale, voire données économiques.

1. L'auteur tient particulièrement à remercier chaleureusement plusieurs officiers de l'armée de Terre ayant demandé à rester anonymes et avec qui il a eu l'occasion de partager leur vision des défis et des opportunités se présentant.

Le renseignement militaire connaît depuis une vingtaine d'années d'importants changements, du fait de l'évolution des technologies et des modes d'organisation, mais aussi et surtout de la mutation de l'art de la guerre. La sortie de la guerre froide a imposé une révision en profondeur de ses structures mais aussi de son champ d'intérêt. Là où l'enjeu principal consistait jadis à déterminer sur une carte de l'Europe occidentale des axes de progression probables des forces du Pacte de Varsovie, il s'agit désormais d'anticiper les actions futures d'un ennemi souvent invisible, voire indéterminé, sur une multitude de théâtres ayant chacun leurs particularités sociopolitiques et militaires.

Par ricochet, que ce soit en France ou ailleurs dans le monde, le renseignement militaire est ainsi devenu un enjeu stratégique et non plus seulement technique et purement tactico-opératif. S'il permet aux chefs en opération de *mieux connaître*, il est également devenu crucial pour le niveau politique, parce qu'il contribue aux décisions de lancement d'une opération, mais aussi parce qu'il est un gage de sûreté des forces et donc de réduction du coût politique d'une opération. En ce sens, le renseignement est devenu une fonction d'appui aussi essentielle que la logistique à la conduite des opérations extérieures contemporaines. Son absence implique la perte de toute liberté de manœuvre.

Nous nous intéresserons prioritairement ici au cas français et ce, sous l'angle du renseignement utile aux actions des niveaux tactique et opératif – en délaissant donc le renseignement militaire stratégique lorsqu'il ne contribue pas à ces niveaux. Dans une première partie, nous examinerons les ressorts conceptuels du renseignement militaire, notamment en rappelant ses fondamentaux et en prenant en compte les espérances portées par la révolution dans les affaires militaires des années 1990. Nous examinerons ensuite quatre catégories de défis – opérationnels, organisationnels, de maintien de la cohérence du cycle de renseignement face à des opérations complexes et technologiques (problématiques de la collecte et de la fusion de données) afin de chercher à comprendre quelle peut être la prospective du domaine.

Le renseignement dans la manœuvre contemporaine

Le renseignement n'est pas l'information, ni même le savoir, mais la production de ce savoir en vue d'éclairer la prise d'une décision[2]. Il peut se décrire de façon classique comme un cycle dans lequel chacune des phases est essentielle à la réalisation du tout. La première étape a trait à la définition d'un *objectif* : comme en toute matière stratégique, il est impératif de savoir ce que l'on cherche. Vient ensuite le temps de la *collecte* qui porte sur le regroupement, par différents moyens, d'informations de toutes natures. La troisième étape est celle du recoupement et de l'*analyse* dans la perspective d'une prise de décision. Enfin, la dernière étape est dédiée à la *diffusion* du renseignement ainsi produit auprès du décideur et son *exploitation* par le commandement et les unités opérationnelles.

Le processus de renseignement ne peut se penser que comme une totalité, tout en étant disséminé aux différents niveaux de conduite des opérations. C'est certes le cas sur le plan stratégique (déterminer les capacités et les intentions d'un pays, par exemple), mais également sur les plans opératif (caractérisation, à l'échelle d'un théâtre, des acteurs, de leurs capacités et intentions, ambiance) et tactique (localisations précises et volume, armement, etc.). Dans ce dernier cas de figure, le renseignement tend, de plus en plus fréquemment, à se confondre avec les fonctions militaires classiques de reconnaissance ou d'éclairage[3] – souvent regroupé sous l'acronyme ISR (*Intelligence, Surveillance, Reconnaissance*). Une information recueillie au contact de l'adversaire au cours d'une mission d'éclairage ou de flanc-garde – normalement utile au chef tactique – peut, de fait, avoir une signification pour le commandant de théâtre. Cet aspect, important dans les opérations contemporaines, présente nombre de défis mais aussi d'opportunités.

La difficulté du travail de renseignement est aussi liée à son objet : le renseignement n'est plus strictement militaire mais est devenu depuis les années 1990 « d'intérêt militaire », ce qui implique d'élargir le champ des

2. O. Chopin et B. Oudet, *Renseignement et sécurité*, Paris, Armand Colin, 2016.
3. Contrairement à l'éclairage, la reconnaissance peut impliquer d'engager le combat.

domaines traités[4]. Si l'on songe à l'évaluation des capacités et des intentions de l'adversaire – une mission historique du renseignement militaire – d'autres aspects ne sont pas moins importants, comme la détermination des différents acteurs (militaires, mais aussi politiques, économiques, sociaux, humanitaires), l'ambiance générale d'un théâtre ou même la culture propre à ce dernier. Par exemple, déterminer le rôle de la rumeur dans les processus d'information – ou de désinformation – des populations locales peut s'avérer essentiel pour la protection des forces. La simple connaissance des coutumes locales est essentielle pour savoir comment aborder les populations comme les élites et savoir ainsi recueillir auprès d'elles des informations utiles, y compris les signaux faibles[5].

Le renseignement dans la guerre

Le rôle du renseignement dans les succès militaires ne va pas nécessairement de soi et a souvent pu prêter à débat, notamment lorsqu'il a conduit à une sous-estimation ou une surestimation de capacités ennemies. L'historien britannique John Keegan estime ainsi que la force et la volonté importent plus dans la réussite militaire que la connaissance de l'ennemi[6]. Ces différents termes ne sont cependant pas antinomiques, d'autant plus que l'évolution des moyens du renseignement a permis d'étoffer les moyens de collecte, contribuant à le crédibiliser mais aussi, parfois, à le rendre central dans l'obtention d'une victoire[7] comme lors des batailles de Tannenberg (1914) ou encore de Midway (1941) – deux cas d'école de l'utilisation des écoutes – mais aussi de la guerre des Six jours ou du débarquement d'Inchon[8].

Au-delà d'un rôle décisif dans la victoire, toujours délicat à cerner, le renseignement est structurellement utile dans la conduite des opérations. Le décodage des transmissions allemandes chiffrées par *Enigma* durant la Seconde Guerre mondiale est devenu un avantage comparatif considérable pour les Alliés, jusqu'au point de constituer une faiblesse vers la fin de la guerre[9]. La bataille des Ardennes de 1944 n'a ainsi pu être anticipée dès

4. Le problème de l'objet ne touche d'ailleurs pas que le renseignement militaire : M. Warner, « Wanted: a Definition of Intelligence», *Studies in Intelligence*, vol. 46, n° 2, 2002, p. 15-22.
5. M. Masson, « Les défis du renseignement militaire », *Sécurité globale*, n° 4, 2008, p. 9-18.
6. J. Keegan, *Intelligence and War: Knowledge of the Enemy From Napoleon to Al-Qaeda*, New York, Alfred Knopf, 2003.
7. Il faut, à cet égard, replacer l'ouvrage de Keegan dans le contexte de la planification de l'opération *Iraqi Freedom*, où le renseignement est vu comme un multiplicateur de force permettant de réduire les ressources allouées à la conduite des opérations.
8. G. Elder, « Intelligence in War: It Can Be Decisive », *Studies in Intelligence*, vol. 50, n° 2, 2006, p. 15-22.
9. Voir notamment R. A. Ratcliff, *Delusions of Intelligence. Enigma, Ultra, and the End of Secure Ciphers*, Cambridge, Cambridge University Press, 2008.

lors que les forces allemandes ont utilisé pour la préparer d'autres systèmes de communication[10]. En ce sens, la citation – souvent moquée – de D. Rumsfeld est pourtant pertinente, en particulier dans un contexte où les moyens de collecte abondent :

> Nous savons [ce] que nous savons ne pas savoir c'est-à-dire que nous savons qu'il y a certaines choses que nous ne connaissons pas. Mais il y a aussi des inconnues que nous ne savons pas. [...] Déterminer cette dernière catégorie a tendance à être le plus difficile.[11]

Ce faisant, l'ancien secrétaire américain à la Défense mettait en évidence le rôle central de la définition d'un objectif dans le cycle du renseignement, mais aussi la difficulté à prendre en compte la veille et les signaux faibles en tant qu'instrument de la lutte contre la surprise.

Le travail de renseignement est une tâche ardue : il s'agit souvent de faire preuve de nuance et d'utiliser des degrés de probabilité dans la rédaction des synthèses, là où le monde militaire tend à privilégier un paramétrage des situations (localisations précises, volumes de forces, etc.). La nature spéculative d'un certain nombre d'analyses s'oppose ainsi à une propension naturelle des décideurs à la recherche de certitudes. Paradoxalement, la première fonction du renseignement militaire, à savoir désépaissir le brouillard de la guerre et réduire l'incertitude, sur les plans tactique, opératif et stratégique, peut également contribuer à rendre les choses moins claires. Répondre à des questions implique d'en voir émerger d'autres. Dès lors, la quête de la certitude ne peut que trouver une réponse asymptotique[12]. C'est l'une des raisons expliquant la méfiance historique des armées, particulièrement françaises, à l'égard du renseignement : il n'a commencé à être introduit dans l'enseignement de l'École supérieure de guerre qu'à partir de 1950 et la Direction du renseignement militaire (DRM) n'a elle-même n'a été créée qu'en 1991[13].

D'autres raisons historiques expliquent cette désaffection française, comme la perception d'une activité déloyale, en rupture avec une perception chevaleresque des armées et du style de guerre français[14]. Ce même style renvoie à « l'école des possibilités » selon laquelle c'est au chef militaire – et non à un officier de renseignement spécialisé – d'imaginer les

10. Voir H. M. Cole, *La grande bataille des Ardennes*, Villance en Ardennes, Omer Marchal, 1994.
11. « DoD News Briefing - Secretary Rumsfeld and Gen. Myer », 12 février 2002.
12. Voir L. K. Johnson, « Introduction » *in* L. K. Johnson (Ed.), *Handbook of Intelligence Studies*, Londres, Routledge, 2007, p. 1-14.
13. J.-C. Cousseran et P. Hayez, *Renseigner les démocraties*, *renseigner* en *démocraties*, Paris, Odile Jacob, 2015, p. 232.
14. Cette vision se retrouve notamment chez Lewal, *Études de guerre. Tactique des renseignements*, Paris, Baudoin, 1881.

mouvements possibles de l'ennemi et d'adapter son dispositif en conséquence. À l'inverse, « l'école des intentions », davantage prônée chez les Anglo-Saxons, implique de n'élaborer une manœuvre que sur la base de minutieux renseignements glanés sur l'adversaire, les capacités de ses forces et leur doctrine. Dans cette optique la dépendance au renseignement est donc plus importante[15].

Toujours sur le plan de l'héritage historique, le manque de valorisation du travail de « deuxième bureau » au sein des états-majors français résulte aussi de sa réputation sulfureuse sur le plan moral et politique. Les souvenirs de l'affaire Dreyfus à la fin du XIX^e siècle – directement liée au renseignement militaire de l'époque – de même que la controverse sur la torture durant les conflits coloniaux, et notamment durant la guerre d'Algérie, auront laissé des traces durables dans l'imaginaire collectif. Cette histoire particulière explique aussi la volonté de la part de la hiérarchie de limiter le renseignement à une dimension avant tout technique, dénuée de portée stratégique ou politique.

La configuration spécifique de la guerre froide a favorisé cette désaffection : l'époque était propice à l'étude des aspects technico-tactiques. Dans cette optique, le renseignement militaire est alors surtout lié à la reconnaissance et à l'éclairage. Le renseignement militaire stratégique existe, bien entendu – en témoigne la spécialisation d'unités comme le 13^e Régiment de Dragon Parachutistes qui prend en 1963 le rôle d'unité spécialisée dans le renseignement « en profondeur », c'est-à-dire derrière les lignes ennemies – mais il renvoie à un théâtre pour l'essentiel connu et porte là aussi sur des questions d'ordre technique.

Tout cela change avec la fin de la guerre froide. Dans le monde en pleine mutation des années 1990 il va soudain falloir combiner le technico-tactique et le politico-stratégique – et ce à l'échelle mondiale. À cette époque, la France va diversifier ses théâtres d'opérations (Moyen-Orient, Balkans, Afrique) et se trouver impliquée dans des conflits où les gains territoriaux ne sont pas nécessairement le but principal, en rupture avec une vision où la défense de la Métropole était au centre des préoccupations. Face à un contexte aussi instable, l'école des possibilités – qui suppose de la part du chef, une connaissance intime de l'adversaire et de ses paramètres, tant sur le plan tactique que politique – s'avère insuffisante. L'engagement sur un théâtre implique alors d'en avoir une vision la plus globale possible, ce qui passe par une production de renseignement unifiée et centralisée. On comprend dès lors mieux la temporalité relativement

15. H. Coutau-Bégarie, « Le renseignement dans la pensée militaire française », *Stratégique*, n° 73, 1999/1.

tardive de l'apparition de la DRM, le passage à une logique interarmées se montrant difficile. Comparativement, la Defense Intelligence Agency (DIA) américaine est mise en place en 1961, trente ans plus tôt – il est vrai, également, que l'investissement américain dans les opérations et déploiements extérieurs était supérieur à celui de Paris.

Cette évolution dans les années 1990 se présente à bien des égards comme un processus de relégitimation du renseignement, surtout aux yeux du monde militaire, et ensuite seulement à l'égard du monde politique. Elle s'est doublée d'un effort pédagogique visant à faire comprendre que son utilisation, y compris à grande échelle et en formalisant/systématisant les pratiques, ne prémunit nullement contre la surprise[16]. Ni panacée, ni recette miracle, le renseignement d'intérêt militaire reste d'abord et avant tout un outil de connaissance et de réduction des incertitudes.

La « *Transformation* » du renseignement

La recherche d'une réduction de l'incertitude comme du brouillard de la guerre a pourtant été au cœur du concept de « révolution dans les affaires militaires » (RMA), dès le début des années 1990, puis de sa projection institutionnelle sous forme de *Transformation*, à partir de 2001. Le domaine ISR apparaît ainsi rapidement, avec l'armement de précision et la furtivité, comme l'un des trois piliers de ladite révolution[17]. La RMA a par ailleurs accru le besoin en renseignement : des forces moins volumineuses, parce que plus technologiquement avancées et plus coûteuses, offrent une couverture géographique moindre, ne permettant plus de mailler les territoires. L'ISR devient alors un facteur de compensation de la lacunarité des espaces de bataille. Dans le même temps, la génération d'effets stratégiques au moyen d'armes guidées de précision accroît d'autant les besoins en renseignement d'intérêt militaire, en particulier dans la grande profondeur adverse.

Ce même domaine du renseignement est par ailleurs étroitement lié à la thématique de la numérisation et de la mise en réseau des forces à travers la figure du C4ISR[18]. La rationalité sous-jacente apparaissait alors comme relativement simple : le couplage d'une variété de capteurs au

16. Sur ces questions : R. Hémez, « L'avenir de la surprise tactique à l'heure de la numérisation », *Focus stratégique*, n° 69, Ifri, juillet 2016 ; C. Brustlein, « La surprise stratégique. De la notion aux implications », *Focus stratégique*, n° 10, Ifri, octobre 2008.
17. Voir par exemple : W. E. Odom, *America's Military Revolution: Strategy and Structure after the Cold War*, Washington D.C., American University Press, 1993 ; W. A. Owens *Lifting the Fog of War,* New York, Farrar Straus Giroux, 2000 ; B. Steed, *Piercing the Fog of War. Recognizing Change on the Battlefield*, Minneapolis, Zenith, 2009.
18. *Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance*.

travers de réseaux interconnectés devait permettre à chaque niveau d'action d'être abreuvé d'informations pertinentes, aidant à l'optimisation des actions conduites. En ce sens, la RMA transposait au domaine du combat interarmées les rationalités initialement observées en combat aérien, au travers d'une séquence « détection-transmission-traitement », dans le ciblage comme la planification des opérations[19].

Pour les tenants de la RMA, la technologie devait donc permettre de rendre transparentes les zones de bataille. Les États-Unis devaient ainsi avoir, à terme, la capacité de détecter 90 % des moyens militaires ennemis[20]. Une telle domination informationnelle devait permettre une action plus rapide, plus précise, avec un degré inédit d'économie des forces, en autorisant un « combat équationnel » où chaque détection positive serait suivie d'une destruction.

Pour séduisante qu'elle fut, cette vision a cependant été assez rapidement remise en cause. Alors que la RMA reposait sur une extrapolation des capacités soviétiques de guerre froide, il est vite devenu évident que les adversaires probables des pays occidentaux adaptaient leurs structures et leurs modes d'action en conséquence. La guerre du Kosovo, en 1999, en a fourni une première démonstration, les forces serbes étant parvenues à limiter considérablement l'efficacité des frappes de l'OTAN du fait d'un usage approprié des leurres[21].

La thématique du C3D2 (*Camouflage, Concealment, Cover, Deception and Deceit*) s'est ensuite répandue dans les débats autour de la « guerre asymétrique » en tant que réponse conceptuelle à la RMA[22]. Plus largement, l'irrégularité est elle-même apparue comme le contrepoint d'une vision techno-déterministe ; qu'elle s'appuie sur les classiques de la guérilla ou sur des évolutions de type « techno-guérilla »/guerre hybride[23]. Les guerres d'Afghanistan et d'Irak sont venues confirmer cette remise en question du renseignement militaire. Le type de conflits auxquels la RMA entendait répondre favorisait le ciblage[24] – la détection et le

19. J. Henrotin, *The Art of War in the Network Age. Back to the Future*, Londres, ISTE, 2016.
20. M. T. Owens, « Technology, the RMA and Future War », *Strategic Review*, Spring 1998.
21. En particulier, seuls 14 chars seront détruits alors qu'ils avaient été définis comme des cibles prioritaires. Sur cette question : D. L. Byman et M. C. Waxman, « Kosovo and the Great Air Power Debate », *International Security*, vol. 24, n° 4, printemps 2000 ; D. G. Press, « The Myth of Air Power and the Future of Warfare », *International Security*, vol. 26, n° 2, Automne 2001 ; T. L. Thomas, « Kosovo and the Current Myth of Information Superiority », *Parameters*, Printemps 2000.
22. Voir J. Henrotin, *La technologie militaire en question*, Paris, Economica, 2008.
23. J. Henrotin, *Techno-guérilla et guerre hybride. Le pire des deux mondes*, Paris, Nuvis, 2014 ; É. Tenenbaum, « Le piège de la guerre hybride », *Focus stratégique*, n° 63, Ifri, octobre 2015.
24. J. R. Ferris, *Intelligence and Strategy. Selected Essays*, Londres, Routledge, 2005.

positionnement de tel effecteur, la localisation de tel PC – au détriment des aspects moins techniques du renseignement.

Or, les conflits à dominante irrégulière nécessitent d'investiguer selon un angle plus large : il ne s'agit plus uniquement de trouver des positions mais également de comprendre des intentions, ce qui est nettement plus complexe[25]. La supériorité informationnelle entendue comme la capacité à localiser des unités ennemies y apparaît comme totalement insuffisante, notamment parce que les combattants au contact doivent pouvoir bénéficier d'un appui et d'une connaissance plus large des facteurs sociaux, politiques ou économiques. Dans le cycle du renseignement appliqué à une opération irrégulière, la fonction d'analyse est ainsi rendue plus difficile : à supposer que cela soit possible, même la détection de l'ensemble des risques et menaces n'est pas la garantie d'un jugement approprié. L'irrégularité charrie *de facto* avec elle des inconnues quant aux acteurs, à leurs intentions et même à leurs capacités. À travers les optiques d'un drone, il est impossible de savoir si une ambulance sert à transporter des blessés, des munitions ou des combattants.

Le renseignement dans pareil cadre pose un certain nombre de défis, et cela d'autant plus que l'on assiste à une diversification de ses moyens avec la croissance continue des informations ouvertement disponibles en ligne qui contribue à décloisonner la séparation traditionnelle entre renseignement technique et humain. Les réseaux adverses/ennemis devenaient eux-mêmes une source et un terrain du renseignement. *In fine*, la figure du « système de systèmes » porte en elle un étiolement des catégories classiques du renseignement, au risque d'une plus grande indistinction entre information et renseignement[26]. Derrière cette évolution se pose évidemment la question du poids des technologies. La RMA fait ainsi la part belle aux drones, satellites, pods et autres systèmes SIGINT (*Signals Intelligence*) – lesquels regroupent l'ELINT (*Electronic Intelligence*) et le COMINT (*Communications Intelligence*). Ce faisant, l'attention se porte sur les systèmes de collecte – dont l'évolution présente néanmoins nombre de défis – au détriment de l'analyse.

Mais, là aussi, la fascination pour le capteur tend à renforcer la fonction de recueil par rapport à celle d'analyse et, par extension, à ce que l'information prenne le pas sur le renseignement. Elle tend également à minimiser les problématiques liées au recrutement, à la formation et à l'utilisation de ressources humaines pertinentes. De ce point de vue, la question n'est sans doute pas, comme on peut trop souvent l'entendre, de

25. Entretien avec un officier français de l'armée de Terre, le 9 septembre 2016.
26. M. Herman, *Intelligence Services in the Information Age*, Londres, Frank Cass, 2001.

savoir si les facteurs humains ou technologiques importent le plus dans la définition des priorités. Les deux sont naturellement nécessaires, mais ils doivent évoluer de manière coextensive, à défaut de quoi des déséquilibres apparaîtraient, entre la surcharge d'informations non recoupées et non analysées d'une part, et des analystes « borgnes » d'autre part.

De tels déséquilibres seraient d'autant plus dommageables que le renseignement d'intérêt militaire a vu ses fonctions évoluer. S'il doit toujours permettre de dissiper, dans une certaine mesure, le brouillard de la guerre (et de la paix[27]) tout en réduisant l'incertitude, il est également devenu un facteur central dans les engagements de forces occidentales. Il permet non seulement d'informer les décideurs politiques, mais il est également devenu le *leitmotiv* de l'évolution des structures de force, la réduction de leur volume devant être compensée par les gains d'efficience permis, entre autres, par les évolutions du renseignement. Ces gains mêlent intimement aspects offensifs – en rendant les forces, du moins théoriquement, plus efficaces – mais aussi défensifs. Elles sont alors dotées d'un « blindage informationnel » accroissant leur sûreté sur le plan opérationnel, mais aussi et au-delà, en réduisant le coût politique associé à un déploiement.

27. G. Rifkind et G. Picco, *The Fog of Peace. The Human Face of Conflict Resolution*, New York, I.B. Tauris, 2014.

Les nouveaux défis du renseignement militaire

La mutation du renseignement militaire n'est pas une problématique récente. Elle avait déjà légitimé la création, en 1976, du Centre d'exploitation du renseignement militaire (CERM), dans la foulée de l'accroissement des pouvoirs du Chef d'état-major des armées (CEMA) à qui il fallait donner une plus large capacité de compréhension[28]. De même, en juin 1992, la création de la DRM avait constitué une nouvelle étape en offrant un interlocuteur unique en matière de renseignement, cette fois au profit du CEMA comme du ministre de la défense. Mais elle a surtout permis d'opérer une concentration des efforts au profit des forces, de coordonner les moyens des armées tout en leur laissant les capacités propres utiles à leurs besoins directs[29]. Vingt-cinq ans après la création de la DRM, cette fonction stratégique doit aujourd'hui faire face à un nouvel ensemble de défis qu'il est possible de regrouper sous trois catégories : organisationnel, de diffusion et technologique. Leur particularité est de se présenter de manière combinée de sorte qu'ils devront nécessairement être abordés de front.

Le défi organisationnel

La DRM n'est pas seule à fournir du renseignement susceptible d'intéresser les armées. C'est évidemment le cas de la DGSE pour les théâtres extérieurs mais aussi, dans un contexte marqué par l'opération Sentinelle, de la DGSI et du Service central de renseignement territorial (SCRT). Reste cependant que les règles arrêtées limitent, dans ce dernier cas, la coopération entre les armées et les services[30]. Sur les théâtres extérieurs, l'évolution du caractère des conflits pose la question de la diversification des besoins en renseignement. Le suivi de problématiques militaires classiques (ordres de

28. C. Fort, « Bref historique des services de renseignement et de sécurité français contemporains », *Revue Historique des Armées*, n° 247, 2007, p. 70-81.

29. Elle rassemble alors le CERM, les deuxièmes bureaux des trois armées, le CIREM (Centre d'interprétation du renseignement électromagnétique), le CFIII (Centre de formation et d'interprétation interarmées de l'imagerie) et l'EIREL (École interarmées du renseignement et de l'étude des langues).

30. É. Tenenbaum, « La Sentinelle égarée ? L'armée de Terre face au terrorisme », *Focus stratégique*, n° 68, Ifri, juin 2016.

bataille, évaluation des savoir-faire) reste nécessaire mais il s'agit aussi d'alimenter en renseignement des opérations de contre-insurrection, de lutte contre le terrorisme à l'étranger ou encore des opérations spéciales. Cet éclatement des configurations de conflits, effectif depuis les années 1990, s'est encore accru depuis 2001 et le basculement dans une lutte ouverte contre les mouvements djihadistes. Dès le début des années 2000, des cellules de coordination du renseignement ont été mises en place sur les théâtres extérieurs.

La dimension massivement irrégulière des conflits des quinze dernières années a mis à rude épreuve le renseignement militaire, en lui opposant un adversaire tactiquement évanescent, dont la « furtivité » reposait moins sur des capacités techniques que sur son lien sociologique avec le terrain humain dont il est issu. L'une des plus célèbres tentatives d'adaptation à ces nouvelles conditions est le rapport « *Fixing the Intel* » sur le renseignement militaire américain en Afghanistan, publié en 2010 par le général Michael T. Flynn – aujourd'hui conseiller à la sécurité nationale du président Trump. Il y proposait notamment de briser la distinction classique entre capteurs et analystes pour les rapprocher dans une logique de spécialisation par théâtre[31]. Cette évolution qui s'est traduite par la mise en œuvre de « Fusion cells » a eu une influence considérable sur nombre de pays de la coalition. Depuis 2014, la DRM a ainsi approfondi ses pratiques antérieures et adopté la logique de « plateau » permettant de rassembler analystes spécialisés, linguistes et officiers de liaison qui peuvent s'appuyer sur les capteurs déployés dans la zone[32].

La mesure n'est pas que d'ordre organisationnel. Elle permet également aux analystes de développer une vision globale d'un théâtre et de ne pas se limiter à leurs zones de confort traditionnelles qui peuvent être source d'une « pensée en tunnel ». La vision doit également permettre de rassembler plus facilement les informations « remontant » du terrain. Ces plateaux ou cellules constituent donc un élément de rééquilibrage à l'égard du renseignement technique : les informations que ce dernier produit y sont certes centralisées mais c'est également le cas pour celles issues des « capteurs humains » sur zone. Simple en théorie, la vision est autrement plus complexe à mettre concrètement en œuvre dès lors que le renseignement militaire est également affaire d'unités déployées sur le terrain, aux niveaux opératif et tactique.

31. M. T. Flynn, M. Pottinger, and P. D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Washington, Center for a New American Security, 2010.
32. B. Connable, *Military Intelligence Fusion for Complex Operations. A New Paradigm*, Santa Monica, RAND Corp., 2012.

Le renseignement dans les forces terrestres

À l'échelon de l'armée de Terre, le modèle « Au contact » a permis de mettre sur pied, en septembre 2016, un commandement du renseignement qui prend la suite de la brigade de renseignement (créée en 1993). Il regroupe plusieurs unités spécialisées et entretient naturellement un lien privilégié avec la DRM. C'est le cas du 2e régiment de hussards (ROHUM), du 54e régiment de transmissions (ROEM tactique), du 44e régiment de transmissions (ROEM stratégique), du 61e régiment d'artillerie (drones *Sperwer*, puis *Patroller* à terme), de la 785e compagnie de guerre électronique (opérations cyber), du 28e groupe géographique, du Centre de renseignement terre (CRT) mis en place en 2016 afin d'exploiter le renseignement au profit des forces terrestres, et enfin du Centre interarmées des actions sur l'environnement (CIAE) en charge des opérations d'influence et d'unités de formation[33]. Ces unités constituent des réservoirs de forces dans lesquels peuvent être prélevées des ressources qui doivent pouvoir être projetées au sein d'un GTIA sous la forme d'un Groupe de recherche multicapteurs (GRM), relevant du niveau division ou brigade. Un GRM est ainsi déployé dans le cadre de l'opération *Barkhane*.

Par ailleurs, à un niveau inférieur, les régiments spécialisés peuvent également nourrir des détachements multicapteurs (DETMuC) ou des sous-groupements de recherche multicapteurs (SGRM). Ce type de structure ad hoc permet ainsi une mise à disposition de moyens, plus lourds, sur un théâtre spécifique[34]. S'y ajoutent des unités ne dépendant organiquement pas du commandement renseignement mais dont c'est pourtant une fonction native : c'est le cas du 13e régiment de dragons parachutistes et d'autres unités de forces spéciales.

Parallèlement aux unités du commandement du renseignement, chaque brigade de la Force interarmes *Scorpion* disposait d'une Batterie de renseignement brigade (BRB), intégrée au régiment d'artillerie et bénéficiant de moyens organiques. Les BRB, dont le concept remonte à 2008, pouvait être détachées au niveau GTIA. Il s'agit d'unités d'une centaine d'hommes regroupés théoriquement en quatre sections :

- Une section de renseignement d'origine humaine à pied ou montée sur des PVP. Elle permettait de rester au contact de la population et d'y recueillir des informations.

33. L'école du renseignement de l'armée de Terre de Saumur et le centre de formation initiale des militaires du rang de Bitche.

34. T. Struye de Swielande, « Le Bataillon de Renseignement Multicapteurs (BRM) », *Défense & Sécurité Internationale*, n° 61, juillet-août 2010.

- Une section de renseignement image, équipée de DRAC (Drones de reconnaissance et d'appui au contact) qui offraient une capacité d'identification d'objectifs ponctuels, à courte portée, en temps réel, de jour comme de nuit. Chaque section était théoriquement équipée de quatre systèmes DRAC, soit en tout, huit drones et quatre stations-sols.
- Une section de renseignement radar à bord de VAB équipés de RASIT (Radar de surveillance des intervalles du terrain). Une telle section pouvait détecter un objectif mobile jusqu'à 30 km[35]. Si le radar n'est pas neuf, il a été engagé au Mali. Un nouveau système, RAPSODIE, était évoqué depuis 2000 et était attendu pour 2010. Depuis, le système MURIN est attendu et devait être commandé en 2016.
- Une section de Renseignement d'origine électromagnétique (ROEM) capable de détecter et de localiser les émissions, voire de les brouiller dans le cas d'adaptation d'un Détachement d'appui électronique (DETAE), de masquage ou de protection. Il sera doté du Système tactique d'écoute, de radiogoniométrie et d'exploitation du spectre électromagnétique (STERNES) lorsqu'il sera disponible.

Depuis l'été 2016 et l'application du modèle « *Au Contact* », les BRB ont été dissoutes[36]. Les brigades s'appuient désormais sur des unités non spécialisées, mais sensibilisées à la recherche élémentaire :

- Les escadrons de reconnaissance et d'intervention de l'arme blindée-cavalerie, qui reprennent à leur compte les missions de renseignement des Escadrons d'Éclairage et d'Investigation (qui avaient été dissous entre 2013 et 2014).
- Les Batteries d'acquisition et de surveillance (BAS), sont subordonnées au régiment d'artillerie des brigades. Elles héritent des drones et des radars issus des anciennes BRB. Les composantes de recherche et d'appui électronique ont, quant à elles, rejoint le 2e RH et le 54e RT.

Il convient d'ajouter à ces moyens présents au niveau brigade la mise en place dans chaque régiment d'infanterie d'une Section d'aide à l'engagement débarqué (SAED) dont l'une des missions est de fournir des renseignements tactiques immédiatement utilisables par leur corps de rattachement[37]. La formation des membres de ces unités, qui sont avant tout d'infanterie, met notamment l'accent sur l'observation, la prise de vues ou encore les langues étrangères au cours de différents types de stages, leur

35. Plus précisément, des piétons jusqu'à 23 km ; des véhicules légers jusqu'à 32 km et des véhicules chenillés jusqu'à 40 km.
36. Échange par courriel avec un officier de l'armée de Terre, 27 janvier 2017.
37. Concrètement, elle compte un VBL et trois VAB dans les régiments d'infanterie.

permettant notamment d'établir des dossiers d'objectifs[38]. Chaque régiment dispose en sus d'un officier et d'un sous-officier spécialisés dans le renseignement de groupement tactique (ORGT). Ils sont le relais entre le bureau renseignement de la brigade et les unités déployées.

Les Sections de reconnaissance régimentaires (SRR), qui étaient intégrées aux compagnies d'appui, ont disparu[39]. Du reste, on pourrait imaginer que le détachement des moyens issus des BAS au niveau des SGTIA constituerait un apport, toutefois délicat à gérer. En effet, les différentes organisations de recueil de renseignement ne fonctionnent pas indépendamment les unes des autres. Le renseignement d'intérêt militaire est un ensemble exigeant une complémentarité des moyens, lesquels ne peuvent évidemment tous être affectés à un SGTIA ou même un GTIA…

Le renseignement dans les forces aériennes et navales

La structure des moyens de renseignement de l'armée de l'Air et de la Marine nationale a également évolué. Elle s'est diversifiée avec l'arrivée des pods Reco-NG/AREOS sur *Rafale* en 2010 mais aussi des drones MALE (*Harfang* en 2008 et premiers MQ-9 en 2013) au sein de l'escadron de drones 01.033 *Belfort*. Sur le plan organisationnel, l'évolution est très significative. D'une part, parce qu'en théorie, toutes les unités (y compris aéronavales) dotées du *Rafale* sont désormais aptes à la reconnaissance, là où auparavant cette fonction était limitée aux seuls *Mirage* F-1CR du 2/33 *Savoie*. D'autre part, parce que les drones signent l'arrivée des logiques de surveillance et de persistance aérienne. Le Centre de renseignement air (CRA), qui exploite et fusionne les données issues des moyens aériens, bénéficie ainsi d'une diversification de ses moyens.

Par ailleurs, la Marine nationale dispose toujours de ses *Atlantique* 2, qui ont montré leur grande utilité en Afrique ou au Moyen-Orient et dont le programme de modernisation est d'ores et déjà établi. De par leur endurance, ces appareils ont joué un rôle similaire à celui des drones MALE. En l'occurrence, ils reçoivent une boule optronique supplémentaire et un nouveau système de traitement de données, en plus d'un nouveau radar et d'un nouveau système de bouées acoustiques.

En ce qui concerne le ROEM, l'enjeu est de taille puisque la France doit maintenir à jour sa connaissance de l'ordre de bataille électronique de

38. Entretien avec un deuxième officier de l'armée de Terre, le 9 septembre 2016.
39. J.-D. Merchet, « Restructurations dans la défense : peu de surprises… », blog Secret Défense, 14 octobre 2014, disponible à l'adresse : www.lopinion.fr.

ses adversaires potentiels, dans un contexte d'émergence rapide de nouvelles menaces sol-air – notamment au regard des problèmes posés par les logiques de déni d'accès (A2/AD). Les *Mirage 2000D* peuvent utiliser les pods ASTAC[40] depuis 2016 tandis que les deux *Transall Gabriel* d'écoute électronique devraient être remplacés par la future Charge universelle de guerre électronique (CUGE) actuellement en phase d'étude de levée de risques[41]. Les deux premiers Avions légers de surveillance et de renseignement (ALSR), des bimoteurs *King Air* 350 dotés de boules optroniques et de systèmes d'écoute, ont par ailleurs été commandés. L'ISR dans la troisième dimension a donc connu des évolutions profondes qui, nonobstant la question des montées en puissance quantitatives (en particulier sur les drones), montrent une réelle adaptation aux opérations contemporaines.

Toujours sur le plan tactique/opératif, la Marine nationale dispose également de systèmes, radars, optiques ou ROEM pouvant contribuer au renseignement sur l'ensemble de ses bâtiments de combat principaux (frégates, sous-marins). S'ils sont d'abord conçus pour le combat naval, ils contribuent également à la collecte du renseignement, en permettant d'évaluer les systèmes de force étrangers. Alors qu'il croisait en mer d'Arabie, le groupe aéronaval a par exemple contribué à la reconnaissance formelle de l'émersion d'un sous-marin nucléaire chinois et ainsi démontré que la Chine avait accru ses aptitudes en la matière. L'arrivée de la nouvelle génération de bâtiments (frégates des classes *Forbin* et *Aquitaine*, sous-marins de classe *Suffren*) implique de ce point de vue un accroissement capacitaire qualitatif.

Sur le plan du renseignement stratégique s'ajoutent également d'autres catégories de systèmes, à commencer par les satellites[42]. La Loi de Programmation Militaire (LPM) 2014-2019 a assuré la continuité de ces programmes. Trois satellites de la Composante spatiale optique (CSO) devraient ainsi être dotés d'ici la fin de l'année 2017 de capteurs optiques et IR d'une résolution jusqu'à 20 cm. La plateforme, issue de *Pléiades*, sera mise en œuvre en coopération avec l'Allemagne, l'Italie, la Belgique, la Grèce, l'Espagne, la Pologne et la Suède. Les coopérations devraient

40. Analyseurs de Signaux tactiques. La nacelle, d'abord utilisée sur les *Mirage F-1CR*, a une fonction ROEM, et plus particulièrement la localisation de radars.
41. M. Friedling (entretien), « Armée de l'Air : des défis capacitaires », *Défense & Sécurité Internationale*, n° 124, juillet-août 2016.
42. Avec deux *Helios II* dotés de capteurs IR et optique et d'une résolution officielle de 50 cm ; deux *Pléiades*, système dual civilo-militaire d'une résolution de 50 cm et d'une fauchée de 20 km. Le statut des quatre ELISA (*Electronic Intelligence by Satellite*) est incertain. Effectuant du renseignement électromagnétique, ils constituaient un démonstrateur considéré comme « pré-opérationnel ».

également permettre un accès structurel à des ressources alliées : avec l'Italie sur COSMO-Skymed (quatre satellites), autre système dual utilisant des radars en bande X et avec l'Allemagne sur les cinq satellites SAR-Lupe dotés de capteurs radars en bande X, et sur leurs successeurs à partir de 2017, les trois SARah. Elle permet également la mise en place d'une capacité ROEM opérationnelle bâtie autour de trois satellites du programme CERES, à partir de 2020.

La Marine nationale dispose quant à elle du navire collecteur de renseignement *Dupuy de Lôme* – dont les spécialistes du renseignement ont une « origine » interarmées – ainsi que des sous-marins nucléaires d'attaque de par leurs systèmes d'écoute électronique (ESM), d'observation et leur possibilité, renforcée sur les futurs sous-marins de classe *Suffren*, de mettre en œuvre des plongeurs.

Le défi du maintien de l'intégrité du cycle du renseignement

Ce rapide tour d'horizon des moyens disponibles pose la question de la coordination de l'ensemble du système et, plus particulièrement, de l'exploitation du renseignement et de sa diffusion auprès des décideurs. Si les moyens de recueil couvrent bien l'ensemble du spectre informationnel, encore faut-il que les données collectées et les analyses qui en découlent puissent être envoyées à temps et utilisées là où elles sont utiles.

Cette question appelle différents commentaires. Le premier est lié aux « remontées » et « redescentes » d'information le long de la chaîne de renseignement. Dans cette optique, l'armée de Terre bénéficie d'un outil baptisé Solution d'aide et d'exploitation du renseignement (SAER) qui se présente comme une base de données essentiellement mise à jour par les forces déployées et dans une moindre mesure par les forces spécialisées. Il n'en demeure pas moins que plusieurs goulets d'étranglements limitent le système, au premier rang desquels l'insuffisance de la bande passante des radios PR4G au vu des besoins en débit toujours plus importants. Les limitations en la matière sont cependant appelées à se résorber avec la future adoption de la radio logicielle CONTACT et du SICS, directement liés au programme Scorpion.

Une autre limitation porte sur la redescente de l'information. Des unités tactiques peuvent bénéficier d'informations ou de prises de vue de systèmes ne dépendant pas de leur niveau en en passant la commande, avec des délais de réception de l'ordre de 24 heures[43]. À l'échelon opératif,

43. Entretien avec un deuxième officier de l'armée de Terre, 9 octobre 2016.

les délais sont évidemment inférieurs. Il n'en demeure pas moins que ce temps de latence réduit la liberté de manœuvre des unités dès lors qu'elles souhaiteraient des renseignements dont elles ne sont pas immédiatement productrices. Selon un autre point de vue, la liberté d'action des éléments tactiques est, de toute manière, réduite dès lors qu'elles opèrent sous le contrôle d'un GTIA, d'une brigade en bonne et due forme, voire de la division. Par contrecoup, l'adaptation de la structure de forces à la morphologie du combat peut être questionnée : les opérations contre-irrégulières menées sur des étendues de plus en plus importantes favorisent ainsi la prise d'initiative des plus bas échelons ; mais ceci n'est possible qu'avec un renseignement approprié, qui s'il est trop volumineux risque de surcharger ses utilisateurs.

Ce dilemme amène à un second commentaire lié à l'appropriation du renseignement d'appui par les différents niveaux. On note à cet égard une tension entre deux modèles. Le premier est celui d'une fonction renseignement déconcentrée où les unités bénéficieraient d'un maximum d'autonomie dans leurs moyens de collecte et d'analyse. C'est certes le cas au niveau de la brigade, en particulier si elle combine BRB et BRM, mais force est également de constater qu'en France, aucune brigade au format du temps de paix n'a jamais été engagée en OPEX et que le modèle théorique n'a jamais été totalement appliqué en opération. En deçà de ce niveau, la densification des moyens de renseignement apparaît complexe, posant le risque d'un alourdissement et d'un accroissement de l'empreinte logistique, comme du coût des acquisitions de matériels. En permettant de réduire les boucles d'interaction « demande/réception », le système a cependant pour avantage de conférer une autonomie plus importante.

Le deuxième modèle envisage *a contrario* des forces à l'empreinte la plus faible possible, certes dotées de leurs moyens organiques de reconnaissance, mais dont le renseignement *stricto sensu* est fourni par un échelon central non déployé. C'est le type de structuration que l'on rencontre le plus souvent dans les forces occidentales et qui autorise une certaine « économie des forces de renseignement », tout en impliquant un travail interarmées – avec l'utilisation des forces aériennes, par exemple. Cependant, cette vision implique des boucles d'interaction particulièrement courtes et donc des systèmes de transmission disponibles en quantité et en qualité. Ce modèle permet d'entrer dans une logique « reachback » où le chef tactique peut s'appuyer directement sur l'analyse fournie par l'échelon central.

Pratiquement, la plupart des solutions opérationnelles sont à l'apex entre ces deux modèles. La tendance naturelle d'un chef opérationnel est de chercher à conserver dans sa main le maximum de moyens pour

dépendre le moins possible d'appuis extérieurs. En ce sens, on peut s'interroger sur la pertinence de la distinction entre les deux modèles évoqués ici. Est-elle encore d'application dès lors que des communications fiables pourraient faire en sorte que le renseignement d'appui ne soit plus considéré comme « relevant d'un autre échelon » mais bien comme étant « déporté », « aplatissant » en quelque sorte la pyramide des niveaux ?

Cette question des modes de diffusion du renseignement amène un troisième commentaire, lié cette fois à la manière dont on envisage le futur des opérations. La zone couverte par chaque unité tend historiquement à s'accroître, tout comme sa profondeur d'action. Le volume d'information exigé est donc amené à croître avec le temps. On pourrait ajouter par ailleurs que l'information peut entraîner une certaine addiction – au risque que son absence, son caractère incomplet ou insatisfaisant provoque une véritable paralysie chez le chef militaire[44].

À ce risque, il faut ajouter celui, bien connu des experts de la numérisation des espaces de bataille, lié à la surcharge informationnelle du chef[45]. Interrogé sur la question des évolutions souhaitées dans le domaine du renseignement militaire, un officier de l'armée de Terre ayant une bonne expérience du combat urbain indiquait que la première devrait toucher au raccourcissement des délais de transmission des renseignements, permettant en retour de dégager du temps au profit de la réflexion[46]. Il indiquait également qu'il était nécessaire de renforcer tous les « deuxièmes bureaux » (J-2 ou L-2), tout en réduisant le nombre de strates et d'échelons. Dans le même temps, le « triage » de l'information devait pouvoir être plus précis, s'approchant de l'optimum du nécessaire à la conduite de chaque action. Plus largement, les premiers retours d'expérience de forces numérisées montrent un raccourcissement de la boucle décisionnelle – en faisant passer une prise de décision majeure de 24 à trois heures[47].

Quel que soit le rôle du renseignement sur l'adversaire, la charge cognitive du chef opérationnel demeure occupée par les informations sur la position de ses propres troupes. En la matière, « renseignement » et « connaissance de son dispositif » ne sont que deux versants du même dilemme informationnel. La disposition de systèmes de *Blue Force*

44. Ce phénomène est parfaitement illustré dans le film de G. Hood, *Eye in the Sky*, 2015.
45. A. K. Cebrowski, « Network-Centric Warfare: Its Origin and Future », *Proceedings*, janvier 1998. Voir aussi N. Friedman, *Network-Centric Warfare: How Navies Learned to Fight Smarter Through Three World Wars*, Annapolis, Naval Institute Press, 2009 ; A. De Neve et J. Henrotin, « La Network Centric Warfare, de son développement à *OIF* », *Stratégique*, n° 86, avril 2006.
46. Entretien avec un deuxième officier de l'armée de Terre, 9 octobre 2016.
47. M. Goya, «Dix ans d'expérience des brigades numérisées Stryker », *Lettre du Retex*, n° 16, CDEF, 16 mai 2014.

Tracking (BFT) permettant une localisation précise des combattants amis aurait pour avantage d'ouvrir la voie au désépaississement du brouillard de la guerre, en particulier une fois affiché sur les systèmes de représentation des positions ennemies/adverses. Les travaux autour de la RMA ont très rapidement souligné la nécessité d'une telle intégration[48], mais elle s'est heurtée jusqu'ici à des goulets d'étranglements techniques. Elle a toutefois été mise en œuvre avec succès – sans être totale – dans les brigades *Stryker* américaines[49]. Mais si les capteurs ne permettent pas une mise en transparence totale du fait de leurs limitations intrinsèques, l'affaire n'est pas que technique. Sa réalisation en France sera d'autant plus complexe que les dernières opérations ont montré le rôle central de coalitions impliquant une immixtion forte, lesquelles charrient avec elles la question de l'interopérabilité des forces coalisées, que ce soit aux systèmes BFT nationaux ou, plus traditionnellement, celle de leur accès aux informations et renseignements produits nationalement.

Ces différentes évolutions conduisent également à s'interroger sur le maintien des séparations traditionnelles entre les catégories du renseignement[50]. Les logiques de numérisation et de partage de l'information tendent en effet à étioler ces distinguos, déjà mis à mal par l'évolution du caractère même des opérations contemporaines. Ainsi, la détermination des responsabilités dans l'attaque chimique de la Ghouta, en Syrie en août 2013, renvoie certes au renseignement d'intérêt militaire, mais ses implications – le lancement potentiel d'une opération militaire – étaient clairement stratégiques et politiques. À l'avenir, la place de plus en plus prépondérante de l'influence et des stratégies médiatiques confère parfois une place stratégique à des renseignements initialement considérés comme tactiques[51]. De ce fait, le renseignement se voit conférer une place importante dans la manœuvre d'influence. Cette évolution, au demeurant, ne fait que refléter le brouillage des niveaux de la guerre[52]. De ce point de vue, le positionnement du CIAE au sein du commandement du renseignement est certainement un choix avisé.

48. Voir, entre-autres, L. Murawiec, *La guerre au XXIe siècle*, Paris, Odile Jacob, 2000.
49. R. Hémez, « L'avenir de la surprise tactique à l'heure de la numérisation », *op cit*.
50. J.-C. Cousseran et P. Hayez, *Renseigner les démocraties*, *renseigner* en *démocraties*, *op cit*.
51. Sur cette question, voir notamment M. Hecker et T. Rid, *War 2.0. Irregular Warfare in the Information Age*, Westport, Praeger Security International, 2009.
52. Lesquels ne se représenteraient plus de manière pyramidale – et voyant se succéder, depuis la base tactique, les niveaux opératif et stratégique avant d'en arriver à la « pointe » politique – mais bien sous un angle matriciel. C. Jean, *Guerra, strategia e sicurezza*, Bari, Laterza, 1997. Voir également H. Coutau-Bégarie, *Traité de stratégie*, Economica, Paris, 2008. Voir également B. Bihan, « Les niveaux de la guerre. Une « *Kriegsanschauung* » américaine » *in* S. Taillat, J. Henrotin et O. Schmitt, *Guerre et stratégie. Approches et concepts*, PUF, Paris, 2015.

D'un côté, l'appui renseignement apparaît de plus en plus nécessaire aux opérations, au point de devenir une condition structurelle d'un engagement, apparaissant ainsi comme un « blindage informationnel ». Mais d'un autre côté, on peut aussi s'interroger sur sa place réelle dans la conduite des opérations. Outre que de nombreux exemples historiques attestent que ce « blindage » a maintes fois été pris en défaut, la question de la confiance qui lui est accordée par les chefs reste pendante. Bien sûr, l'imagerie en temps réel est une denrée très clairement perçue comme utile – d'autant plus qu'elle est appelée à être mieux représentée[53] – mais il ne s'agit là que d'une extension des modalités classiques de reconnaissance par l'intermédiaire technologique. La véritable interrogation porte plutôt sur des renseignements moins immédiatement matériels – intentions, réseaux interpersonnels, etc. – sur lesquelles l'emprise intellectuelle de l'officier est moins immédiate et nécessitant une confiance en l'échelon supérieur. En la matière, quand bien même les évaluations seraient disponibles et accessibles en temps réel, aucune réponse ne semble pouvoir être assurée autrement que par l'actuel système de notation par lettres et chiffres en fonction de la qualité de la source et du renseignement…

Les défis technologiques liés à la collecte

Si la question de la diffusion de l'information et de la numérisation est pour partie d'essence technologique, elle n'est pas le seul défi de cette nature se posant aux forces. On peut les classer en deux catégories : la première a trait à l'évolution des moyens de collecte, tandis que la deuxième est liée à la fusion des données et à leur représentation.

Sur le plan de la collecte, les moyens utilisés sont encore appelés à s'étoffer du fait de l'intégration de systèmes initialement réservés au ciblage. Sur ce plan il convient d'emblée de préciser que les vecteurs aériens sont aujourd'hui le premier axe de développement du renseignement. Les opérations en Afghanistan, puis en Libye, ont ainsi vu l'utilisation d'appareils de combat dotés de pods de désignation – aux optroniques de plus en plus puissantes – comme « systèmes de reconnaissance de poche » ou comme systèmes de surveillance à proprement parler (missions dites NT-ISR[54]). L'utilisation de terminaux vidéo comme le ROVER (*Remote Operations Video Enhanced Receiver*) américain permet aux combattants d'avoir accès, en temps réel, à

53. Le SICS permettra de géoréférencer les informations, tout en les horodatant. H. Perot, « L'info-valorisation dans Scorpion », *Fantassins*, n° 36, printemps-été 2016.
54. *Non-Traditionnal Intelligence, Surveillance, Reconnaissance*.

l'imagerie produite par les pods[55]. L'outil est utile pour confirmer une position dans le cadre d'un appui-feu, mais il peut offrir également la possibilité de disposer d'un véritable système de surveillance ou de reconnaissance, au profit d'une unité ou de son échelon supérieur[56]. À moyen terme se profile également la perspective pour des unités tactiques de disposer directement d'images satellites[57].

Au-delà se pose la question de la diversification des fonctions de systèmes déjà opérationnels ou sur le point de l'être. C'est en particulier le cas dans le domaine des drones. Une voie d'évolution consiste en la miniaturisation des drones, particulièrement aériens (dès lors qu'ils s'affranchissent naturellement des obstacles), qui sont susceptibles d'être utilisés par l'infanterie, conférant à cette dernière un plus grand degré de conscience situationnelle[58]. L'enjeu, à ce stade, n'est pas uniquement lié à la machine en elle-même, mais également à l'automatisation de ses fonctions – déchargeant cognitivement son opérateur – et à son aptitude à être intégrée dans des essaims fournissant une « bulle informationnelle », en plus de l'aptitude à reconnaître ou surveiller une zone donnée.

Une autre piste porte sur l'intégration de drones aériens depuis la mer, permettant d'établir des réseaux de surveillance aérienne discrets et persistants – à l'instar des orbites de drones MALE déjà conduites aujourd'hui – notamment en utilisant des drones à changement de milieu pouvant être mis en œuvre depuis des sous-marins, comme le *Blackwing* américain ; ou plus classiquement des drones lancés depuis des bâtiments de combat de surface[59]. La question de la mise en œuvre de tels réseaux par la voie aérienne, notamment en utilisant l'aviation de transport, capables de larguer des essaims de drones, est également revenue récemment sur le devant de la scène avec les propositions de la DARPA[60]. Les ballons-drones constituent également une possible évolution, permettant de disposer à

55. O. Zajec, « Le "paradigme ROVER" : paradoxes de la standardisation en coalition », *Défense & Sécurité Internationale*, n° 61, juillet-août 2010.

56. Du moins, lorsque l'appareil a pour mission d'appuyer l'action d'une unité : les optroniques étant stabilisées, ce type d'utilisation n'est pas problématique. Elle implique cependant une planification aérienne en bonne et due forme dès lors que la vitesse de transit d'un appareil de combat ne le rendrait pas disponible longtemps au profit de l'unité qui en bénéficierait.

57. Au début des années 2000, le Pentagone avait ainsi lancé le programme TacSat, ensuite annulé après plusieurs lancements.

58. P. Langloit, « Robotique terrestre : le grand désenchantement ? », *Défense & Sécurité Internationale*, n° 111, février 2015.

59. J. Henrotin, « Puissance navale et puissances navales : quo vadis ? », *Défense & Sécurité Internationale*, hors-série n° 50, octobre-novembre 2016.

60. J. Henrotin, « La troisième *offset*, les réseaux et la guerre au futur antérieur », *Défense & Sécurité Internationale*, n° 123, mai-juin 2016.

bon compte de « pseudolites » (pseudo-satellites) ayant pour avantage de rester en position fixe et d'emporter une bonne masse de capteurs[61].

Dans tous les cas de figure, il s'agirait de généraliser la persistance de la surveillance – augurant ainsi d'une véritable « occupation aérienne[62] ». Ce type de rationalité permet également un armement et la possibilité de compresser encore davantage le cycle F2T2EA (*Find, Fix, Track, Target, Engage, Assess*). Ce type de dispositif fait écho aux « complexes de reconnaissance-frappe » de la théorie soviétique des années 1980 ou, plus récemment, à des concepts tels que la *fire-ant warfare* développée dans le cadre de la RMA qui imaginait une force « dominée par des escouades de capteurs, d'émetteurs et de microprojectiles[63] ». En tout état de cause, les systèmes robotisés sont appelés à jouer un rôle important en la matière.

Un autre axe de développement concernant les drones est la diversification des capteurs, ce qui implique des efforts non seulement dans le domaine de la miniaturisation, mais aussi des capacités de traitement informatiques, en particulier pour ce qui a trait aux systèmes optroniques. Actuellement, les drones sont limités par un « effet-paille » impliquant de savoir « où » orienter les capteurs. Pourtant, une fauchée sur de grands-angles est techniquement possible. Introduit en 2011, le programme américain *Gorgone Stare* avait ainsi pour but de positionner des pods permettant une vision panoramique à 360° sur des drones MQ-9 *Reaper*. Mais les liaisons de données ont rapidement été saturées par les informations transmises et les logiciels mis au point afin d'extraire les informations les plus pertinentes n'ont jusqu'ici jamais fonctionné.

Certes, le milieu aérien devrait demeurer le principal fournisseur du renseignement militaire, en revanche c'est le champ du cyber qui connaît aujourd'hui la plus forte croissance. Depuis le début des années 1990, le développement exponentiel de l'internet a complètement changé la donne en matière de Renseignement en source ouverte (ROSO) en mettant à disposition de gigantesques volumes d'information d'ordre technique (manuels, données) ou analytiques (articles, notes et rapports de

61. G. Boutherin et C. Pajon, « Drones 2025 : la relève de la garde », *Défense & Sécurité Internationale*, hors-série n° 10, février-mars 2010 ; J.-J. Mercier, « Hélidrones et dronigeables : un marché en pleine évolution », *Défense & Sécurité Internationale*, hors-série n° 18, juin-juillet 2011.

62. C. Fontaine, « L'occupation aérienne : le chaînon manquant à l'obtention de la maîtrise opérative dans les conflits de basse intensité », *Défense & Sécurité Internationale*, hors-série n° 42, juin-juillet 2015. Voir également J.-C. Noël, « Puissance aérienne : quelles avancées ? », *Défense & Sécurité Internationale*, hors-série n° 18, juin-juillet 2011 et J. Henrotin, « De l'identité fluide des opérations aériennes », *Défense & Sécurité Internationale*, n° 113, avril 2015.

63. M. C. Libicki, « The Small and the Many » *in* J. Arquilla et D. Ronfeldt (dir.), *In Athena's Camp: Preparing for Conflict in the Information Age*, Santa Monica, RAND Corp., 1997, p. 198.

recherche, etc.)[64]. Le ROSO a une influence directe sur le renseignement stratégique mais pose aussi la question de ce qu'est une source ouverte. Si le recours à des moteurs de recherche grand public est au cœur de l'image traditionnelle du ROSO, des algorithmes de recherche spécifiques sont également mis au point, permettant d'optimiser l'accès aux sources disponibles[65]. C'est par exemple le cas d'OSIRIS (Outil de surveillance et d'information sur les relations inter-sud), programme focalisé sur le Moyen-Orient dans les domaines comme l'armement ou le nucléaire et conçu par la CEIS au profit du ministère de la Défense[66]. Au-delà se pose la question d'algorithmes permettant de chercher dans le « deep web » des informations qui ne sont pas nécessairement protégées mais qui nécessitent des techniques de recherche plus complexes[67].

Le cyber ouvre, au demeurant, d'autres perspectives. Au même titre que le renseignement et les opérations spéciales entretiennent des liens étroits, le renseignement dans le cyberespace ouvre également la voie à des actions directes. Qu'il s'agisse de cyberattaque ou de cyberdéfense, le renseignement y apparaît comme la capacité la plus importante. Corrélativement, plusieurs questions se posent : comment organiser les formations pour garantir le capital humain ? Quelle structure adopter au sein des armées de façon à répondre efficacement aux besoins de chacun sans disperser les efforts ? Quels liens établir entre DRM, DGSE et DIRISI ? D'autre part et dans le même temps se pose la question des actions dans le domaine de l'influence, en particulier sur des réseaux sociaux, devenus eux aussi des enjeux de puissance. Quel doit être le rôle des États ? Faut-il y intervenir, y compris par la force, notamment quand des mouvements de foule sont instrumentalisés et risquent de porter atteinte à la sécurité des armées engagées en opération[68] ?

Avec les réseaux sociaux, les objets connectés constituent l'autre grande source d'information qui contribue à alimenter la problématique

64. W. K. Wark (dir.), *Twenty-First Century Intelligence*, Londres, Routledge, 2013; O. Chopin et B. Oudet, *Renseignement et sécurité*, *op cit.* ; M. M. Lowenthal, *Intelligence: From Secrets to Policy*, Londres, SAGE, 2014 ; J. Henrotin, « *Intelligence, the first defense?* Quelques observations sur la guerre de l'information dans son rapport à la surprise stratégique » *in* D. Ventre (dir.), *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Paris, Éditions Hermès Lavoisier, 2010.

65. S. Chahan et N. K. Panda, *Hacking Web Intelligence. Open Source Intelligence and Web Reconnaissance Concepts and Techniques*, Waltham, Syngress, 2015 ; R. Layton et P. A. Watters (Eds.), *Automating Open Source Intelligence. Algorithms for OSINT*, Waltham, Syngress, 2015.

66. A. Schwartzbrod, « Osiris tient le sud à l'œil », *Libération*, 10 mars 2011.

67. T. Singletary, « Dark Web and the Rise of Underground Networks » *in* M. Blowers, *Evolution of Cyber Technologies and Operations to 2035*, New York, Springer, 2015.

68. P. K. Rozumski, « The Rise of Social Media and Its Role in Future Protests and Revolutions » *in* M. Blowers, Evolution of Cyber Technologies and Operations to 2035, New York, Springer, 2015.

dite du « big data » qui contribue à faire du cyber un champ majeur de l'avenir du renseignement militaire[69]. Les objets connectés offrent de réelles opportunités en opérations, en permettant par exemple d'accéder aux systèmes de vidéosurveillance d'une ville et donc de disposer rapidement d'un grand nombre de capteurs, y compris dans les zones tenues par un adversaire. Les flux de données transitant par les réseaux GSM sont également susceptibles de fournir de précieux renseignements. Cette évolution illustre d'ailleurs la convergence croissante entre guerre électronique et cyber[70]. Ces opportunités sont naturellement toutes aussi valables pour l'adversaire – et ce d'autant plus que les forces occidentales ou russes sont de grandes consommatrices de communications.

L'usage de moyens de communication mobiles augure également de possibles manœuvres couplant renseignement et *State-building*, la reconstitution des réseaux permettant à la fois d'écouter des forces adverses (ou des témoins neutres de leur action) et de participer à des efforts de réhabilitation des infrastructures. Dans tous les cas de figure, le défi technique touche en particulier aux capacités de captation et surtout du traitement – nécessairement automatisé – de gigantesques volumes de données, ce que l'on imagine aisément consommateur en ressources.

Toutes ces perspectives technologiques posent naturellement la question de leur financement et de la génération d'une structure de force appropriée. Nombre de programmes sont d'ores et déjà en cours d'acquisition, principalement dans le domaine des drones, mais pas uniquement, qu'il s'agisse des systèmes *Patroller* qui viendront remplacer les *Sperwer* du 61e régiment d'artillerie à partir de 2018 ; de la commande du quatrième système MQ-9 en décembre 2016, qui portera à douze le nombre de drones *Reaper* disponibles à partir de 2019 ; des réflexions autour du remplaçant du DRAC et de la CUGE ; de l'achat en 2016 de deux ALSR ; de la mise en œuvre des programmes déjà engagés dans les domaines navals ou spatiaux[71] ; ou encore de la modernisation des 54e et 44e régiments de transmission, matériels divers d'observation, etc.

Les questions liées à l'ISR semblent désormais bien prises en compte dans les programmations budgétaires et ne devraient plus impliquer de batailler pour prouver leur nécessité – ce qui n'a pas toujours été le cas, de sorte que 80 % du renseignement utilisé durant l'opération Harmattan

69. D. Fletcher, « Internet of Things » *in* M. Blowers, *Evolution of Cyber Technologies and Operations to 2035*, New York, Springer, 2015.
70. S. Dossé et A. Bonnemaison, *Attention : cyber ! Vers le combat cyber-électronique*, Paris, Economica, Paris, 2014.
71. Moyens ESM des FREMM et des futures FTI (Frégate de taille intermédiaire) pour la Marine nationale ; future composante spatiale optique et CERES pour le domaine spatial.

était d'origine américaine. En dépit de ces efforts, le retard accumulé est encore grand : l'armée de l'Air italienne, pourtant moins engagée dans des opérations, disposera d'ici 2020 de plus de drones MALE que l'armée de l'Air française et ceux-ci seront armés[72]. De même, la British Army aura à sa disposition, après la mi-2017, 54 drones tactiques *Watchkeeper* soit, en l'état actuel des planifications, 40 de plus que l'armée de Terre. La question se pose donc de savoir si les efforts consentis, bien réels, sont suffisants.

Les défis technologiques liés à l'analyse

Au-delà de la question des capteurs, une autre problématique a trait au processus de fusion des données et à leur traitement automatisé. Cette question est certes liée à la cohérence du cycle du renseignement mais également à son appropriation par l'utilisateur final. De nombreux progrès ont été réalisés en la matière et trouvent aujourd'hui une concrétisation au travers du GEOINT (*Geographical Intelligence*), auquel la DRM accorde une grande attention[73]. Le procédé consiste à combiner des couches de renseignement (imagerie, capteurs, ROHUM, ordres de bataille, etc.) et des données géographiques (voies de communication, bâtis, reliefs, etc.) afin de les représenter spatialement[74]. La prise en main du renseignement devient alors bien plus ergonomique, offrant une vision plus claire d'une situation donnée.

Les défis en la matière ne manquent pas. Si un Centre de renseignement géospatial interarmées (CRGI), dépendant de la DRM, a été créé à Creil en janvier 2015 et a connu une montée en puissance assez rapide, il s'agit également de rattraper un retard marqué « de plus de vingt ans sur les Américains, et de dix ans sur les Britanniques et les Allemands[75] ». Par ailleurs, le développement de cette capacité, et notamment la mise à jour en temps réel des représentations produites, se heurte, une fois de plus, aux limitations françaises en matière de bande passante des communications spatiales, mais aussi à la question du nombre de capteurs disponibles, de l'intégration des données issues d'un éventuel BFT, de l'automatisation du traitement des données ou encore des capacités de calcul informatique nécessaires.

72. Au total, 19 machines (7 RQ-1, 6 MQ-9 et 6 P.1HH).
73. C. Fontaine, « Théorie, processus et organisation de la manœuvre des capteurs », *Défense & Sécurité Internationale*, n° 87, décembre 2012.
74. P.-D. Régnier, « Le renseignement géospatial à la française », *Défense & Sécurité Internationale*, hors-série n° 37, août-septembre 2014,
75. P. Boulanger, « En France, le renseignement géospatial a 20 ans de retard », *Le Point*, 22 septembre 2015, disponible à l'adresse : www.lepoint.fr. Notons néanmoins la création en 2003 d'une première Section d'Appui Géographique (SAG).

La question du cyber et du *big data* se pose également en matière d'analyse : les évolutions technologiques promettent ainsi de pouvoir utiliser des algorithmes susceptibles de naviguer dans de gigantesques masses d'information pour y relever des renseignements pertinents, y compris dans les zones de bataille[76]. Cet enjeu n'est pas sans conséquence sur les capacités de calcul dont auront besoin les spécialistes du secteur – dont la qualité et la quantité sont par ailleurs un enjeu de taille. Cette perspective ouvre également des interrogations sur l'intégration aux produits des données qui seraient issues d'alliés ou de coalisés ; ou, plus classiquement, sur la sécurité informatique des produits. Une intrusion malveillante pourrait en effet avoir des conséquences catastrophiques comme par exemple des tirs fratricides suite à la manipulation de cartes[77].

La valeur militaire donnée à ce « renseignement intégral » dépendra de l'attitude des chefs militaires à son égard. De ce point de vue, autant un rejet de ce type de solution serait aussi dommageable qu'une sacralisation qui induirait une vision « en tunnel » amenant à déconsidérer toute information au prétexte qu'elle n'a pas été captée. La « mise en transparence » des espaces de bataille dépendra alors autant des nouveaux systèmes et de l'usage de la géolocalisation que de la prise en compte, à l'échelle humaine, de la possibilité que tout n'ait pas été détecté. Le problème, cependant, n'est pas spécifiquement lié au renseignement géospatial : il traverse toute l'histoire du renseignement militaire.

76. C. P. Atwood, « Activity-Based Intelligence: Revolutionizing Military Intelligence Analysis », *Joint Forces Quarterly*, n° 77, avril 2015, disponible à l'adresse : http://ndupress.ndu.edu.
77. Ce qui constituerait la transcription moderne des actions menées par les Israéliens durant la guerre du Kippour. Ces derniers s'étaient alors infiltrés dans les réseaux radio de l'artillerie égyptienne pour y injecter des coordonnées de tir de batteries.

Conclusion

Au cours des deux dernières décennies, le renseignement militaire en appui aux opérations a connu, en France comme ailleurs, un processus d'adaptation particulièrement dynamique. Cette adaptation est-elle pour autant satisfaisante ? D'un point de vue opérationnel, les déficits sont encore nombreux et relèvent principalement des volumes disponibles : la qualité est rarement problématique, mais c'est bien souvent la quantité, en particulier des ressources humaines, qui fait défaut. Le nombre de capteurs est également problématique, notamment au vu de la dépendance au renseignement américain, que ce soit dans le cadre de l'opération *Barkhane* ou de *Chammal*. Dans le renseignement comme dans d'autres secteurs des armées, la France souffre de capacités trop souvent « échantillonnaires ». Ce saupoudrage, qui ne laisse véritablement aucun trou capacitaire, permet cependant d'imaginer une vraie remontée en puissance. Cette dernière nous paraît nécessaire pour plusieurs raisons :

- Sur le plan tactique : la réduction des formats, conséquence du coût de la modernisation, implique que les forces déployées puissent avoir une plus grande efficience. Or, cette dernière peut notamment s'acquérir par une connaissance plus fine d'une situation, permettant de mieux rentabiliser chaque action. Le renseignement est ainsi devenu le premier appui d'un chef militaire et le préalable absolu à toute action ;
- Sur le plan opératif : la dilatation des espaces d'opérations implique mécaniquement l'augmentation du volume de renseignement. Ce dernier permet ainsi de rentabiliser un certain nombre d'outils, liés notamment aux feux dans la profondeur. Ajoutons que la conduite d'opérations contre-irrégulières impose une diversification mais aussi une densification des moyens du renseignement ;
- Sur le plan stratégique : la plupart des retours d'expérience soulignent que des déficits en renseignement ont été observés, impliquant une dépendance à des sources extérieures. S'il est trivial de le rappeler, le renseignement est l'un des premiers instruments de la souveraineté dans le domaine militaire ;
- Sur le plan politique intérieur : si les opérations extérieures sont conduites pour l'intérêt de la nation, les intérêts vitaux sont rarement en cause, de sorte que la protection de la force est un paramètre essentiel pour le soutien politique à la poursuite des opérations. De ce

point de vue, le renseignement agit de plus en plus comme un « blindage informationnel » ;

- Sur le plan des relations interalliées : le renseignement est un levier de puissance permettant d'offrir, au sein des coalitions où la France est engagée, un avantage comparatif qui peut être unique. Il ouvre ainsi la voie à la vision d'un combat couplé où l'apport français porterait plus particulièrement sur des renseignements. L'engagement de drones MALE dans l'opération Barkhane est ainsi clairement perçu comme la marque d'une aide de poids par les États africains alliés.
- Sur le plan international : de plus en plus, le renseignement est utilisé en appui aux décisions d'engagement de la force, les légitimant aux yeux de la population, mais aussi de la scène internationale.

Par-delà ce rôle accru dans les opérations, le renseignement connaît une mutation de plus en plus marquée vers un décloisonnement de ses catégories classiques : si les outils sont perçus comme tactique ou stratégique, leur production est susceptible de concerner tous les niveaux. Si le renseignement géospatial en est une concrétisation, cette tendance pose également plusieurs questions, notamment dans l'établissement des périmètres des différents services. Elle deviendra probablement de plus en plus saillante dès lors que le domaine du cyber est appelé à impliquer aussi bien la DGSI, que la DGSE ou la DRM. À cet égard, il y a certainement une réflexion à conduire, y compris sur les plans juridiques et organisationnels, qui dépasse cependant le cadre de cette étude. D'autres questions y renvoient plus directement. C'est le cas de la définition des priorités capacitaires, qui sont potentiellement légions dans un environnement de ressources contraintes.

La question du nombre des capteurs – particulièrement celui des drones, essentiels sur le plan opératif – se pose ainsi en même temps que la montée en puissance du renseignement géospatial, trop longtemps déconsidéré. Ces deux aspects sont également cruciaux, tout en étant coextensifs et formant ainsi les deux faces d'une même pièce. En la matière, les solutions ne pourront venir que d'un progrès réel en matière de partage capacitaire et de coopérations entre alliés – Européens notamment elles-mêmes conditionnées à une juste répartition des ressources budgétaires.

ifri
institut français
des relations
internationales