Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2016)
Heft: [2]: Numéro Thematique Aviation

Artikel: L'hybridité dans la troisième dimension : Menaces et problèmes
Autor: Grand, Juilien
DOI: https://doi.org/10.5169/seals-781508

Un Hawker *Hunter* décolle de l'autoroute. Afin d'augmenter notre liberté de manœuvre, un certain niveau de rusticité reste de mise face à une menace hybride.

Stratégie

L'hybridité dans la troisième dimension – Menaces et problèmes

Maj EMG Juilien Grand
Rédacteur adjoint, RMS+

Une contribution de cette revue thématique aviation se propose de définir la menace hybride, d'en poser les problèmes et de proposer quelques pistes de solution. *Quid* de la troisième dimension? De prime abord, l'aviation militaire ne semble pas devoir faire face à un adversaire hybride. Et si la réalité était autre? Petit tour d'horizon.

Existe-il une menace hybride dans la troisième dimension?

Même si des groupes non étatiques, tels le mouvement des Tigres de libération de l'Îlam Tamoul (LTTE), ont réussi à mener des opérations aériennes, certes limitées, l'irruption d'un tel adversaire dans les cieux européens demeurent peu probable. De manière générale, les forces aériennes occidentales se préparent plutôt à affronter des appareils de combat de cinquième génération, voire plus, et misent avant tout sur des avantages technologiques pour l'emporter. Cet état de fait pourrait néanmoins forcer un opposant disposant de peu de moyens aériens à recourir à des formes d'action hybride pour contrer une force aérienne trop puissante.

Les récents conflits démontrent ce qui est maintenant devenu une réalité; sans supériorité aérienne, il est extrêmement difficile voire impossible de manœuvrer. Le recul de l'EI en Syrie a débuté avec le soutien aérien russe apporté au régime de Bachar El-Assad; la Libye du colonel Kadhafi s'est effondrée après que l'OTAN ait pris le contrôle des cieux libyens. Ainsi, un état qui ne dispose pas des moyens nécessaires pour établir ou contrer la supériorité aérienne adverse pourrait trouver un ersatz dans des formes d'action hybride.

Quels risques pour les Forces aériennes?

Si cet adversaire potentiel ne peut établir sa supériorité aérienne, alors peut-être peut-il influer sur nos opérations aériennes pour empêcher leur conduite et ainsi contrer l'établissement de notre contrôle sur l'espace aérien. La menace hybride se distingue par le fait qu'elle est déjà active bien avant le début des opérations militaires ouvertes. L'adversaire a donc tout loisir de chercher et trouver nos failles afin de pouvoir, le moment venu, empêcher la conduite des opérations aériennes et miner la crédibilité des Forces aériennes et de notre gouvernement au moment où ceux-ci nécessiteraient une pleine confiance de la part de la population.

Si les Forces aériennes représentent l'élément mobile, rapide et capable de concentration des forces sur le champ de bataille, celles-ci dépendent néanmoins fortement d'installations fixes, telles les bases aériennes où les stations radar militaires fixes qui sont, la plupart du temps, très vulnérables. De même, la conduite centralisée et la mise en réseau des senseurs et des effecteurs créent de nouvelles vulnérabilités dans le domaine cyber. La première menace qui pèse ainsi sur nos Forces aériennes, dans un cadre hybride et qui pourrait se concrétiser dès aujourd'hui, se manifeste dans la sphère de l'information et du renseignement. De nombreux renseignements pourraient intéresser un adversaire hybride potentiel.

La liste suivante, non exhaustive, permet de se rendre compte de l'étendue de la menace:

- Organigramme du personnel des BA et de la composante volante;
- Organisation de la sûreté des BA et des emplacements FA;
- Emplacements des stations radars militaires fixes et mobiles ainsi que des aides à la navigation aérienne;
- Organisation logistique des BA, y compris fournisseurs externes et emplacements pour le maintien en condition opérationnelle du matériel volant;
- Structure de la conduite et processus en vigueur;
- Logiciels utilisés pour la préparation et la conduite des opérations;
- (...).

Les possibilités découlant de la collecte de tels renseignements sont quasi infinies, allant de la pression sur des personnes-clés d'une BA à la destruction physique, par du sabotage, des installations de navigation aérienne, en passant par l'infiltration de firmes et sociétés chargées du ravitaillement des BA.

L'espace électromagnétique pourrait également offrir un autre moyen d'action privilégié à un adversaire hybride. En effet, les opérations modernes tendent à dépendre de plus en plus des moyens informatiques et de leur mise en réseau. Durant la dernière guerre israélienne au Liban, Tsahal est parvenu à effacer les échos de ses appareils sur les radars de la défense aérienne syrienne. Avec un soutien étatique, cette possibilité technique pourrait donc bien s›ouvrir à n'importe quel groupuscule. A l'époque où les opérations aériennes sont ordonnées via le système FIS LW, on ne peut que mal imaginer les conséquences si un adversaire parvenait à y intégrer de fausses informations ou alors venait à gommer et insérer des informations erronées dans la *Recognized Air Picture* de l'AOC.

Un scénario pour résumer

Afin de pouvoir mettre une image concrète sur les menaces évoquées plus haut, traçons un scénario fictif afin de comprendre la portée que pourraient atteindre certaines de ces actions hybrides. Suite à diverses pressions et alors que le jeu diplomatique n'est pas parvenu à calmer une crise, un état s'apprête à mener des opérations contre la Suisse. Celui-ci ne dispose que de Forces aériennes limitées, dans certains domaines inférieures aux nôtres. Il sait donc qu'il lui sera difficile d'établir sa supériorité aérienne sur le champ de bataille, condition sine qua non pour mener des opérations terrestres. Quelques jours avant que celui-ci ne passe à l'action, deux raids coordonnés, l'un sur une base aérienne, l'autre sur la firme chargée de la maintenance de nos appareils de combat, permettent de détruire environ un tiers de notre flotte. Les informations glanées depuis une dizaine d'année ont permis d'enfoncer rapidement le système de sécurité de la BA, tandis que l'entreprise a été infiltrée depuis plusieurs années par des personnes qui se sont fait engager comme employés. Ces actions ont été planifiées et menées par des groupuscules totalement autonomes, soutenus en sous-main par l'état qui nous fait face. Tout lien avec celui-ci demeure néanmoins, sur un plan strictement juridique, au rang d'hypothèse, ce qui empêche de facto une réaction en bonne et due forme. C'est d'ailleurs une action de ce type, menée sur une base américaine, qui avait engendré les plus grosses pertes d'appareils américains lors de la dernière guerre en Afghanistan.

Quelques jours plus tard, une action cybernétique paralyse la centrale des opérations aériennes, rendant ses systèmes informatique inopérants. Sur une base aérienne, où est cantonné un autre tiers de nos moyens aériens, tout le personnel, y compris navigant, tombe malade. La première action a pu être menée depuis l'étranger par un groupe payé par l'état qui nous fait face, alors que sur la base aérienne, un autre groupe est parvenu à empoisonner la nourriture servie au personnel afin de rendre celui-ci inopérant. Ainsi, en quelques jours, deux tiers de nos moyens aériens seraient paralysés, le tout par des actions ne nécessitant pas d'énormes besoins militaires, sinon une créativité sans limite pour trouver des failles et les exploiter en conséquence. Les conditions sont alors réunies pour commencer une poussée militaire « traditionnelle. »

Dans une telle situation, notre gouvernement se trouverait en position de faiblesse, décrédibilisé et peut-être même contraint et forcé de négocier avec notre opposant, avant même qu'un coup de feu ne soit tiré. Bien sûr, un tel scénario demeure hypothétique et science-fictionnel, mais il démontre que des modes d'actions hybrides pourraient influer rapidement et de manière importante sur les opérations aériennes, y compris dans le cadre d'un conflit étatique et face à des forces armées symétriques, sans qu'un immense effort logistique ne soit nécessaire. De telles menaces, comme les actes de sabotage, existaient bel et bien avant l'apparition du terme hybride, ce que l'on appelait alors la cinquième colonne. Mais l'émergence des nouvelles technologies de l'information et de la communication ont créé de nouvelles failles et, surtout, de nouvelles possibilités pour un éventuel opposant, sans compter l'effet psychologique que comportent de telles actions.

Quelles réponses ?

Ce constat étant posé, quelles mesures pourraient contrer ces éventuelles menaces ? Il serait tout d'abord nécessaire d'assurer la protection de l'information à tous les niveaux et dans toutes les situations. Trop souvent, le militaire suisse se montre naïf face à la protection de l'information, pensant que de toute manière personne ne s'intéresse à des informations qui semblent de peu d'importance ou que chaque interlocuteur est pavé de bonnes intentions. Nos prédécesseurs avaient érigé en manière de vivre le TOZZA, à savoir le fait de ne rien divulguer sur leurs emplacements, missions, troupes, etc... Dans le cadre d'une menace hybride, chaque information a un prix, le domaine de l'OPSEC, pour reprendre une nomenclature OTAN, gagne donc en importance. A l'heure du tout numérique, où chaque soldat dispose d'un téléphone portable, il serait plus qu'urgent de sensibiliser tout un chacun aux conséquences de toute fuite d'information, y compris si celle-ci venait à se produire par inadvertance. Une règlementation supplémentaire par le biais d'une directive ou d'un ordre n'apporterait, à notre sens, aucune avancée dans le domaine. Sans sombrer dans la paranoïa, cette thématique devrait être traitée systématiquement lors de chaque exercice et à chaque échelon, ce qui permettrait certainement de rendre chaque militaire conscient de ses actes ou de ses inattentions. A titre d'exemple, on pourrait démontrer à la troupe, lors d'un exercice, les informations que l'on peut glaner par le biais de social engineering. De la sorte, des modes d'actions hybrides seraient rendues bien plus compliquées pour un adversaire potentiel.

Une autre piste de solution pourrait se trouver dans la décentralisation des moyens. En ne mettant pas tous ses œufs dans le même panier, on rend ainsi le travail plus

difficile à un éventuel adversaire hybride. Cette solution porte néanmoins en elle un grand désavantage; celui de multiplier les besoins en personnel de sécurité, dès lors que plus d'emplacements doivent être assurés. Avec une armée disposant de 100'000 hommes, les éléments chargés de la sécurité des BA risquent de se réduire à la portion congrue. Toutefois, avec un peu de créativité et d'imagination, il est rapidement possible de procéder à des mesures de déception afin de brouiller les pistes et ainsi rendre impossible toute action de sabotage, voire en limiter la portée. En tous les cas, et cela va de pair avec la créativité évoquée plus haut, il demeure important de garder un certain niveau de rusticité dans le fonctionnement de notre composante aérienne. Si l'apport des multiplicateurs de force, tels que la Link16 ou le système FIS LW ne sont pas débattus, il est vital de pouvoir tout de même entretenir les savoir-faire nécessaires pour opérer dans un mode dégradé et à partir de bases aériennes sommaires. Ce faisant, il est possible de réduire la portée d'actions hybrides, menées déjà avant le début des opérations aériennes à proprement parler.

Enfin, il nous semble plus que jamais vital de procéder à du *red teaming* lors des exercices et autres préparatifs. Le principe même du red teaming est de se faire l'avocat du diable et de tenter de penser à l'impensable. Il s'agit avant tout d'adopter un mode de pensée ouvert à la critique et à la remise en question. Le *red teaming* ne cherche en effet pas des coupables, mais trouve des failles avant que l'adversaire ne puisse en faire de même. De la sorte, il est possible de mettre des dangers en évidence et d'y remédier par un processus itératif. Ces red team reprendraient, dans nos exercices, le rôle joué par la menace hybride, complétant ainsi l'engagement de marqueurs. En devançant ainsi un adversaire potentiel, il serait possible de lui couper l'herbe sous le pied, en remédiant à une faiblesse avant même que celle-ci ne doive être payée par le prix du sang.

Pour résumer

La menace hybride pèse également sur les opérations aériennes, même si cela ne semble pas évident de prime abord. Limitée essentiellement aux sphères de l'information et électromagnétique, il n'en demeure pas moins que celle-ci pourrait poser de sérieux problèmes à nos Forces aériennes en cas de conflit, respectivement limiter grandement sa liberté de manœuvre. Les réponses doivent être pensées maintenant pour les conflits de demain. Il demeure plus que vital d'augmenter le niveau de la protection de l'information à tous les échelons, de corriger nos failles par le biais de red teaming et de préparer cadres et soldas à pouvoir continuer à travailler dans un environnement dégradé, dans lequel tous les outils habituels ne sont plus à disposition. Garder des œillères face à ce type de menace signifie peut-être que nos appareils ne pourront même pas prendre l'air lors d'un prochain conflit.

J. G.

Une centrale d'opérations aérienne. La mise en réseau offre de nombreux avantages mais présente également de nouvelles vulnérabilités.