Les opérations aériennes et le cyber : de l'analogie à la synergie

Par le général Denis Mercier

Les analogies sont dangereuses. En voici une monumentale : les opérations aériennes et les cyber-opérations sont analogues, par nature. À ceci près que cette affirmation relève de faits et non d'intuition. Quelques exemples :

- L'élément aérien et le cyberespace couvrent le monde entier, en partageant la même perméabilité.
- Identifier une action maligne dans les méandres cybernétiques est comparable à l'interception d'un aéronef au comportement douteux au sein de la circulation aérienne générale : une aiguille dans une meule de foin.
- Tous deux exigent des alertes ultra-réactives et des cycles de décision en temps réel. Le cycle décisionnel le plus rapide l'emporte.
- A l'instar de la guerre aérienne, c'est la nature des cyber-cibles qui détermine le niveau si l'opération en cours relève du niveau tactique ou prend une envergure stratégique.
- L'air fut le champ de bataille insoupçonné du 20e siècle. Le cyber est en passe de devenir le nouveau lieu d'affrontement au 21e siècle.

Au-delà d'une simple analogie, les opérations Air et Cyber développent une relation d'interdépendance qui s'accroît de jour en jour. Les moyens cyber sont indissociables de la troisième dimension (satellites, antennes, ondes), tandis que les opérations aériennes, historiquement à la pointe de la technologie, utilisent de manière intensive les réseaux informatiques. Du fait de cette interdépendance, afin de combattre dans les airs et dans le cyberespace, l'armée de l'Air a dû s'approprier la nature de ce nouvel environnement stratégique. Forte de cette redéfinition, elle s'engage dans la conception d'une planification opérationnelle qui prend en compte le cyber dans toutes ses missions aériennes, intégrant réciproquement la dualité potentielle inhérente à tout type de cyber-activité. Cette approche intégrée est à la source du système de combat aérien futur.

L'armée de l'Air et le cyber

Il convient d'abord d'examiner la façon dont l'armée de l'Air comprend l'environnement cyber au sein duquel elle évolue. Si elle dispose de réseaux en propre, elle est aussi connectée informatiquement aux autres armées, directions et services, aux autres ministères, voire à certaines industries. Elle échange également avec ses partenaires internationaux et ses alliés, en bilatéral comme dans des forums, et donc des réseaux, multinationaux. Reprenant l'analogie liminaire, ces interconnexions multiples exigent des procédures similaires à celles qui autorisent le transit ou les opérations d'un espace aérien souverain à un autre. Il n'y a en effet pas d'utilisation de l'espace aérien possible sans le

Publié in ***Res Militaris*** (http://resmilitaris.net), **hors-série** "**Cybersécurité**", **juillet 2015**

contrôle de cet espace. Et la surveillance des systèmes d'information fait partie des manœuvres dans le cyberespace. Mais ce contrôle représente également la principale difficulté. Il est physiquement impossible de suivre toutes les pistes radar ou informatiques. La clef réside dans la définition d'un seuil de détection acceptable, capable de détecter les signaux faibles tout en rejetant une majorité de fausses alarmes. Et dans les deux domaines Air et Cyber, l'objectif demeure le même : préserver l'activité opérationnelle.

Au cours d'une mission de combat aérien, la règle d'or est la suivante : détecter, identifier, classifier. Alignée sur des règles d'engagements précises, appuyée sur une base de données renseignement robuste, cette chaîne logique peut conduire à l'assistance, l'abandon ou la neutralisation de la piste radar qui a provoqué le décollage en alerte. L'importance de cet algorithme apparemment simple (détection, identification, classification, règles d'engagement, *data-base*) trouve toute sa pertinence dans le domaine cyber. La redondance et la résilience des moyens représentent d'autres qualités partagées : dans le domaine des opérations aériennes ou cyber, il faut avoir un "*backup plan*".

Mais la capacité principale du succès de nos campagnes aériennes actuelles est la capacité d'assurer en permanence le commandement et la conduite des opérations. C'est la mission du Centre national des opérations aériennes à Lyon, qui assure la gestion centralisée 24h/24, 7 jours/7 de toutes les missions de l'armée de l'Air, que ce soit dans le cadre de la protection du territoire national ou des opérations extérieures. Les cyber-crises nécessitent des structures similaires afin de répondre en temps réel aux cyberattaques, que ce soit en réaction ou en anticipation. L'analogie a assez duré, il est temps de trouver des synergies, tant les opérations aériennes ou cyber sont désormais indissociables.

Sans renier le "*figthing spirit*" de ses héros aviateurs, la campagne aérienne doit être imprégnée de "*cyber spirit*" depuis sa conception, en passant par sa préparation, jusqu'à son exécution. Réciproquement, une cyber-opération pourrait reprendre avec bonheur les processus de planification opérationnelle Air afin d'aboutir à un processus de *cyber-targeting*, afin d'obtenir des cyber-effets compatibles avec l'établissement de règles de cyber-engagement.

Air et Cyber : des analogies aux différences

Dans cette recherche passionnante de similitudes, il serait toutefois dangereux d'oublier des divergences entre les armes aériennes et informatiques. La première différence réside dans la dualité du cyber, qui concerne aussi bien le matériel que l'information véhiculée. À l'opposé d'une bombe ou d'un missile tels que nous les employons sur les théâtres d'opérations actuels, une cyberattaque même ciblée présente de grandes chances de causer des dommages collatéraux dans les réseaux qu'elle utilise. De plus, contrairement aux effets des armements traditionnels, ce sont des dégâts difficiles à anticiper et à évaluer.

Une autre différence concerne le facteur temps. Pour la puissance aérienne, la réactivité se mesure en minutes (2 à 7 minutes pour le décollage d'un avion de chasse en

alerte) et la précision en secondes (le défilé aérien du 14 juillet donne une bonne idée de la minutie temporelle requise tous les jours en opérations). Au contraire, le délai de cyber-impact est souvent difficilement maîtrisable. En effet, le développement d'une bombe logique (logiciel espion, virus, cheval de Troie…) nécessite des délais assez longs pour disposer de tous les détails techniques du système cible, en étudier profondément les ramifications, découvrir ses vulnérabilités, réaliser la bombe logique et connaître ses effets (y compris induits), définir et mettre en œuvre un moyen d'installer furtivement cette bombe au bon endroit.

L'impact du milieu influence grandement les rapports de force entre les adversaires potentiels. En effet, la fluidité de l'air rend l'affrontement "symétrique" et la loi du plus fort prévaut. À l'inverse, dans le domaine cyber, l'environnement s'accompagne d'un potentiel asymétrique important, pour lequel ce n'est pas toujours le plus fort qui a l'avantage. Par ailleurs, le géo-référencement – c'est-à-dire l'identification certaine et la localisation précise de l'attaquant – des systèmes cyber est complexe. L'attribution d'une attaque n'est pas toujours aisée et rend d'autant plus difficile une riposte adaptée et étayée par des règles d'engagement robustes.

Enfin, l'arme cyber est souvent un fusil à un coup : dès que le virus devient actif, il se trouve exposé et à un moment ou à un autre, formellement identifié puis éradiqué. Ce côté éphémère diverge des tactiques de combat aérien dont certaines remontent aux as de 1914 : nous les utilisons encore car elles sont toujours efficaces, malgré leur longévité.

Synergies

Notre défi est donc bien de nous intéresser à la relation entre les deux champs opérationnels afin d'exploiter leur complémentarité, plutôt que de s'abandonner à une réplication irréfléchie et contre-productive de leurs modes d'action. Il s'agit dès lors de penser le cyber en appui d'une opération aérienne afin d'en amplifier certains effets : arrêter les radars au moment du passage d'un raid aérien, coupler une cyberattaque à des actions non-cinétiques ou des forces spéciales, protéger nos propres forces déployées ou non d'une contre-offensive cyber… À rebours, on peut imaginer une opération aérienne en appui d'une manœuvre cyber interarmées : quelle option tactique offrirait la destruction ciblée par air de nœuds de communication en support d'une opération de désinformation ou de blocage de réseaux informatiques ?

L'éventail des possibilités offertes par cette synergie air-cyber doit être exploré. Mais la réflexion prospective sur les capacités futures doit aussi s'en nourrir. S'éloignant des logiques d'acquisition de plateforme, trop réductrices, elle doit se concentrer sur l'aspect systémique du nouvel espace stratégique ainsi défini. Il importe de raisonner dès aujourd'hui à partir des systèmes d'information, systèmes de commandement et de conduite des opérations, systèmes de données, systèmes de sécurité.

Aussi, pour le système de combat aérien futur que l'armée de l'Air conceptualise, le mot-clef est bien "système". Car il ne s'agira ni d'un avion piloté, ni d'un drone, mais d'un

système de systèmes intégrant, au sein d'un véritable *Cloud*, des senseurs et des effecteurs de différentes natures et de différentes générations. Son épine dorsale sera un noyau C4ISTAR (*Command, Control, Communications, Computers, Information/ Intelligence, Surveillance, Targeting Acquisition and Reconnaissance*). Système fédérateur, il obéira également à une logique distributive : diffusion des informations fusionnées en une image synthétique (*Recognized Air Picture*) à l'ensemble du réseau, mais aussi distribution en temps réel de la capacité de contrôle opérationnel des moyens à partir du système le plus pertinent.

Cette approche peut inspirer une architecture à la fois robuste et ouverte vis-à-vis de systèmes cybernétiques, qui s'y adapterait. Résilient et cohérent, ce système de systèmes cyber serait fondé sur la constitution d'une *Recognized Cyber Picture* à vocation analogue à la *Recognized Air Picture*. Les deux seraient d'ailleurs liées de manière dynamique au sein du commandement et de la conduite des opérations afin d'en optimiser les effets.

Conclusion

Ceci n'a rien d'une fiction. La synergie air-cyber est la réalité opérationnelle d'aujourd'hui. Ce qui est en jeu est la réalisation de nos missions, en prenant en compte une dimension cyber de plus en plus prégnante, que ce soit pour la maîtrise de la sécurité de nos systèmes ou pour son intégration dans des modes d'action offensifs nouveaux. Enfin, la définition du bon niveau de souveraineté et d'interopérabilité avec nos partenaires sera déterminante pour nos futures coopérations en matière de cyber.