# Armée de l'Air : le combat numérique au cœur des opérations


L'efficacité acquise en France en matière de cyberdéfense, civile et militaire, résulte de la nécessité d'assurer, notamment, la protection du territoire et le succès des opérations aériennes.

Ce thème a fait l'objet d'un colloque organisé, le 1er juillet 2015 à Paris, par le Centre d'études stratégiques et aérospatiales. Y sont notamment intervenus : le général Denis Mercier, chef d'état-major de l'armée de l'Air ; le vice-amiral Arnaud Coustillière, officier général à la cyberdéfense au ministère de la Défense ; le général de division Joël Rode, inspecteur adjoint de l'armée de l'Air ; le général de division Jean-Christophe Zimmerman, commandant en second la défense aérienne et les opérations aériennes.

**Les enjeux nationaux.** Le ministère de la Défense entretient des relations avec ceux des Affaires étrangères et de l'Intérieur, en vue d'une vision globale au profit des armées conventionnelles et des forces spéciales, explique l'amiral Coustillière. Les institutions mafieuses améliorent leurs performances dans l'espace numérique et recrutent ainsi des jeunes qui ne trouvent pas d'emploi. L'organisation djihadiste Daech y diffuse sa propagande. En conséquence, les armées doivent intégrer ces éléments à tous les niveaux de renseignement de

théâtre, des commandos sur le terrain au Centre de planification et de conduite des opérations à Paris. Déjà, le Centre d'analyse de lutte informatique défensive réagit vite, par exemple le piratage éventuel des données de conduite de tir d'un système d'armes ou les cyberattaques contre la chaîne de commandement. En la matière, la vigilance fait partie de la préparation opérationnelle de chaque unité. L'entraînement cyberdéfense au niveau du commandement opératif (théâtre) se fait aux Écoles militaires de Saint-Cyr Coëtquidan. Fin 2014, la Direction générale de l'armement (DGA) a conclu un accord général de partenariat avec la Région Bretagne et une douzaine d'universités, d'écoles d'ingénieurs et d'institutions de recherche sur la cyberdéfense. D'ici à 2018, elle disposera de 500 ingénieurs informaticiens. Enfin, la sécurisation de la montée en puissance de la cyberdéfense, avec obligation de résultats, implique de garder les compétences des personnels.

**Les opérations aériennes.** Planification, programmation et conduite rythment les opérations aériennes, indique le général Zimmerman. La préparation opérationnelle des équipages prend du temps. La planification implique de partager les données entre de nombreux acteurs, dont les systèmes de communications utilisés sont plus simples ou plus complexes. La programmation exige la diffusion d'informations à d'autres partenaires en France et dans le monde, en vue de conduire des interventions en temps réel. En métropole, le Commandement des opérations aériennes mobilise de nombreux contributeurs avec des systèmes connus. Il doit pouvoir les projeter sur un théâtre extérieur et armer des systèmes de circonstances, selon les coalitions. Il doit être capable de remplir des missions là et quand elles sont demandées, avec des partenaires militaires… et civils ! Conduire une opération pour atteindre le résultat recherché ne se réduit pas aux seuls aspects techniques, estime le général Zimmerman. Il faut savoir jusqu'à quel point un système de communications de données est utilisable et jusqu'où il est remplaçable par un autre. Ainsi, un réseau plus ou moins classifié doit être interconnectable avec d'autres dans un délai contraint, sans pour autant compromettre ses fonctions opérationnelles. Cela dépend d'une connaissance en amont des systèmes, plus anciens ou plus avancés.

**Évaluation et prévention des risques.** L'armée de l'Air recense les entreprises susceptibles d'assurer la protection de ses personnels et matériels face aux attaques informatiques. Elle peut ainsi croiser les informations pour évaluer et maîtriser les risques, indique le général Rode. Ainsi, l'avion de chasse Rafale et le

système de défense SAMP/T (sol/air moyenne portée/terrestre) Mamba disposent de systèmes informatiques dédiés et protégés pour éviter une prise de contrôle malveillante. Les tests de pénétration de ces systèmes, pour en évaluer la fiabilité, nécessitent de mobiliser des ingénieurs pendant plusieurs heures et d'investir des millions d'euros pour les protéger. Selon le général, il en va de l'image de l'armée de l'Air. Celle-ci doit également évaluer au quotidien les fragilités potentielles, liées à un autre type de fonctionnement des systèmes de communications.

**L'esprit « cyb'air ».** Les espaces numérique (cyber) et aérien présentent des similitudes, à savoir l'absence de frontières et leur fluidité autour de la terre, explique le général Mercier. Les systèmes de communications dépendent de plus en plus du cyber, qui permet de réagir en temps réel. Ainsi, les opérations aériennes en Afrique sont conduites à partir de la base de Lyon-Mont Verdun, avec des images en trois dimensions de la situation sur le terrain. A l'avenir, les systèmes de communications, de plus en plus centralisés, devront être décentralisés pour les opérations. Ainsi, la base de Mont-de-Marsan gèrera les différentes plates-formes de commandement et de conduite. Parallèlement, des « smart bases » de gestion du soutien et de la protection seront mises sur pied et interconnectées. La logique actuelle des plates-formes interconnectées évoluera vers leur interconnexion sélective avec les réseaux de communications, de recueil d'informations et de conduite des opérations. Dans dix ans, tout sera géré en temps réel. Le commandement pourra savoir, par les capteurs, comment attaquer : avec des Rafale plus rapides ou des drones de combat plus furtifs. Toutes les plates-formes disposeront de ce système de commandement et de conduite. Mais en cas de problèmes, il faudra pouvoir couper un morceau de l'architecture centralisée du commandement et le déléguer à des gens capables de le traiter. Le « cyb'air », alliance du cyber et de l'aéronautique, correspond à un état d'esprit de l'armée de l'Air, explique son chef d'état-major : modernisation des capacités, simplification des structures et ouverture sur le monde civil. Le succès des futures missions de combat repose sur le partage des bonnes pratiques, estime le général Mercier.

**Loïc Salmon**

Cyberdéfense militaire : DEFNET 2015, exercice interarmées à tous les niveaux

Armée de l'Air : engagement opérationnel intense et réforme en profondeur

Armée de l’Air : création d’un « centre de guerre aérienne »

*Selon le Livre blanc 2013 sur la défense et la sécurité nationale, la capacité informatique offensive, associée à celle de renseignement, concourt à la posture de cybersécurité. Elle contribue à la caractérisation de la menace et à l’identification de son origine, permet d’anticiper certaines attaques et de configurer les moyens de défense en conséquence. Elle enrichit la palette des options possibles à la disposition de l’État. Elle comporte différents stades, plus ou moins réversibles et plus ou moins discrets, proportionnés à l’ampleur et la gravité des attaques. En matière de cyberdéfense, la France va approfondir ses relations avec la Grande-Bretagne et l’Allemagne. Elle soutient la mise en place d’une politique européenne de renforcement de la protection contre le risque cyber des infrastructures vitales et des réseaux de communications électroniques.*