Zeitschrift: Revue Militaire Suisse
Herausgeber: Association de la Revue Militaire Suisse
Band: - (2020)
Heft: [2]: Numéro Thématique 2

Artikel: L'intégration du domaine cybernétique à la 3e dimension
Autor: Grand, Julien
DOI: https://doi.org/10.5169/seals-913964

Le temps du *hacker* qui agit dans l'ombre n'est pas révolue. Mais il est grand temps que les armées parviennent à intégrer ces outils dans un véritable ensemble opératif.

Aviation

L'intégration du domaine cybernétique à la 3e dimension

Lt col EMG Julien Grand
Rédacteur adjoint RMS+

Avec l'arrivée des appareils de nouvelle génération, l'importance du spectre électromagnétique prend encore plus d'importance dans la conduite de la guerre aérienne. Ces développements créent bien entendu de nouvelles possibilités mais aussi de nouveaux risques. Comme nous avions pu l'écrire dans les colonnes de la *RMS*, il y a quelques mois, l'un des développements futurs en matière de guerre aérienne tend d'ailleurs à faire de l'espace électromagnétique un terrain-clé pour la supériorité aérienne.

Le cybernétique dans la guerre aérienne

Les armées de l'air de par le monde tentent en conséquence d'investir le domaine cybernétique pour en faire un usage dans la 3e dimension. Les enjeux sont nombreux, surtout en raison de la présence du cyberspace dans toutes les activités liées à la 3e dimension, comme l'a affirmé le général Willam Shelton, ancien commandant de l'US Air Force Space Command. La base de toute opération aérienne est représentée par la capacité à pouvoir établir la situation aérienne. Ce fait n'est pas nouveau puisque, lors de la bataille d'Angleterre déjà, la RAF avait pu tenir la dragée haute à une Luftwaffe supérieure en nombre notamment grâce à son réseau de radar qui lui permettait de créer des efforts principaux. Au jour d'aujourd'hui, la nouveauté réside dans les distances qui s'allongent de plus en plus avec des armes aériennes capables de frapper à plusieurs centaines de kilomètres. En conséquence, des systèmes AEW ont été mis en place. L'arrivée des avions de 5e génération pose la question de leur maintien puisque chaque appareil, à l'avenir, devrait avoir une conscience situationnelle améliorée de par la connectivité entre tous les appareils présents sur le théâtre d'opération. La mise en place de ce système de systèmes engendre toutefois des besoins en liaisons de données ou le recours accru à des satellites, augmentant encore les intrusions possibles dans le système adverse. On peut, à ce titre, parler d'une intégration aéro-cyber. Ces mêmes appareils modernes requièrent de plus le conditionnement de masse de données énormes en vue de préparer une mission. Les systèmes de guerre aérienne actuels ne seraient en effet que de bien pâles guerriers sans leurs bases de données qui permettent de faire face, notamment, aux mesures de déception et de brouillage électronique adverses ou encore de calibrer les armes en fonction de l'adversaire et de l'objectif. On peut considérer que ces plateformes ont une existence non seulement physique mais également cybernétique. Par exemple, on estime que le fonctionnement du F-35 a nécessité la programmation de 8 millions de lignes de code pour fonctionner. Ce tableau serait incomplet sans l'évocation de l'utilisation faite du cybernétique dans le fonctionnement des infrastructures nécessaires à la conduite aérienne, que cela soit une base aérienne ou alors une centrale d'opération aérienne. Cette dernière se trouve par ailleurs bien souvent à des milliers de kilomètres de l'endroit où sont employées les forces.

De par le monde

Déjà en 2006, les Etats-Unis avaient annoncé la création d'un *Air Force Cyber Command* sur la base de la 8th *Air Force*. Ce commandement recevait alors les missions suivantes : maintenir et protéger la cyber-infrastructure de l'USAF pour assurer un accès constant et sûr pour chacun de ses membres et pour protéger les données ; défendre la cyber-infrastructure pour éviter tout brouillage et autre piratage informatique ; attaquer les infrastructures adverses. Depuis, l'unité a muté pour devenir la 16th Air Force, soit une force aérienne commandée par un général trois étoiles et complètement consacrée à la gestion du cyberespace dans la 3e dimension. La France a également créé un commandement consacré à ce domaine ou, pour être plus précis un centre d'excellence cyberdéfense aérospatiale rattaché à l'école de l'air. La raison de cette création est explicitée dès la page d'accueil du site consacré à ce pôle d'excellence : « *La cyberdéfense est clairement devenue une priorité stratégique pour le Ministère des Armées, raison pour laquelle l'École de l'air a créé un centre d'excellence en cyberdéfense du*

Un CAOC américain, centre névralgique pour toute conduite d'opérations aériennes. Une intrusion cybernétique dans l'un de ses systèmes pourrait avoir de grandes conséquences.

milieu aérospatial». La France poursuit ainsi le but de former les décideurs de demain en matière de guerre aérienne aux défis posés par la cyberdéfense. La RAF a elle créée une *Joint Cyber Unit* pour faire face aux développements dans ce domaine et les publications de son *Air Power Review*, depuis renommée *Air and Space Power Review*, tendent à considérer de plus en plus le thème de l'intégration cybernétique.

Des capacités pour la troisième dimension

Il est possible de distinguer entre trois types d'opérateur cybernétique dans la 3e dimension. Tout d'abord, tout personnel qui opère des systèmes et des armes fonctionnant sur la base des nouvelles technologies. Viennent ensuite les spécialistes cyber à proprement parler, chargés de la conduite des opérations cybernétiques défensives et offensives et, enfin les commandants et les officiers d'état-major qui doivent être à même de planifier des opérations aériennes en intégrant le domaine cyber et ses effets. Il est nécessaire de disposer d'opérateurs qui soient capables de considérer à la fois la sphère aérienne et cybernétique car toute pensée en silo engendrerait une perte d'efficacité. Toute opération future se devra de considérer les vulnérabilités et les chances cybernétiques. Si cela compte ici en particulier pour les opérations aériennes, les opérations au sol sont également concernées. Comme nous pouvons le constater plus haut, les profils différents qui font usage des outils cybernétiques nécessitent également des besoins différents. Une approche multidisciplinaire est donc nécessaire pour répondre aux différents besoins en matière cybernétique mais également pour être à même de répondre avec succès aux vulnérabilités qu'induisent les systèmes de nouvelle génération.

Car tout est une question de vulnérabilités. Pour user de meilleures capacités en matière cybernétique, y compris de manière offensive, il faut pouvoir trouver la faille ou le talon d'Achille cybernétique de l'adversaire. Pour ce faire, il est nécessaire que le fait cybernétique ne soit pas seulement considéré pour lui-même mais bien qu'il trouve une intégration opérative voire tactique pour déployer ses effets. En matière de guerre aérienne, cette intégration et ses effets pourraient même survenir en amont d'une opération, rendant peut-être caduque l'utilisation de certains effets cinétiques. Si l'on se remémore l'attaque de Stuxnet sur les centrifugeuses iraniennes de Natanz, alors il n'est pas difficile d'imaginer qu'une attaque cybernétique puisse paralyser le réseau électrique d'une base aérienne ou interrompe les aides à la navigation ou toute autre infrastructure sans lesquelles les opérations aérienne deviennent compliquées dans le meilleur des cas et impossibles dans un scénario catastrophe. Seule l'imagination humaine met une limite aux capacités de nuisance que pourraient utiliser un adversaire pour gêner ou empêcher une opération aérienne.

Le terrain-clé à l'avenir passe donc par une intégration du domaine au sein des forces aériennes dans le monde. Il ne s'agit d'avoir la haute main sur ce nouveau champ de bataille et cela ne remet aucunement en cause les commandements cyber mis en place dans les différentes armées mais bien de parvenir à une intégration dans

le sens du mot *Joint* ou *Combined* afin de parvenir à synchroniser les effets défensifs et offensifs cybernétiques à la manœuvre aérienne. Les Anglais parlent même d'intégrer ces effets dans le cycle de planification standard aérien et de consacrer un chapitre de l'ATO (*Air Tasking Order*) aux activités cyber. Au niveau stratégique, le département de la défense américain a par ailleurs déjà mis en place une ligne d'opération cybernétique. Elle a trouvé son expression notamment lors de la campagne contre la Serbie. Les systèmes de défense anti-aériens serbes ont été leurrés par de fausses pistes introduites de manière électronique dans le système, ce qui a permis donc de supporter directement la campagne aérienne. Cela aurait été possible en utilisant une faille dans la connectivité du système C2 serbe. Dans la même veine, la maîtrise de l'information a été utilisée, lors de frappes sur des quartiers-généraux, pour informer les occupants et leur permettre d'évacuer les immeubles. Cela n'a pas été fait pour tous les quartiers-généraux, jetant ainsi la suspicion entre les rangs serbes, le personnel de bâtiments ayant été frappés sans évacuation suspectant les autres de collaborer avec l'OTAN. Ces exemples démontrent l'avantage à intégrer cette ligne d'opération dans la planification et la conduite de la guerre aérienne. Une dominance dans ce domaine permettant en effet d'obtenir un avantage conséquent voire de garder ou gagner l'initiative qui est souvent décisive. A ce titre, citons le Wing Commander de la RAF Paul Withers : « *Le succès de la puissance aérienne au début de son deuxième centenaire est fortement lié à l'atteinte de succès dans le domaine cyber.* »[1]

La ligne entre domaine cybernétique, guerre de l'information et opérations électromagnétiques est toutefois ténue à tirer. C'est peut-être ici la raison pour laquelle l'intégration n'est pas encore totalement réalisée dans les armées occidentales. Un regard du côté de la Russie pourrait débloquer la situation en raison de l'approche culturelle différente à ce sujet. La doctrine russe ne distingue pas de domaine cybernétique à proprement parler mais rassemble les domaines cités plus haut dans ce qui est nommé espace de l'information. Ce dernier inclut autant les ordinateurs que le processus cognitif humain de gestion de l'information. Cette vision permet alors de rassembler les opérations psychologiques et cybernétiques sous le même toit puisque c'est le champ cognitif de l'adversaire qui est considéré et au centre de la planification de l'opération.

Et l'avenir ?

A l'avenir, les nouveautés en matière de technologie de l'information continueront d'influencer la conduite de la guerre aérienne. L'arrivée de l'intelligence artificielle pose ainsi de nombreuses questions qui poussent également dans le sens d'une intégration cybernétique au domaine aérien. Car, dans la course au développement de l'IA, la question de savoir qui la développera en premier est certes centrale, mais celle de savoir qui l'utilisera au mieux semble encore plus pertinente. Certainement que l'IA amènera trois attributs particuliers en matière de guerre aérienne : une amélioration de la vitesse cognitive, la possibilité de traiter de plus gros volumes d'information, l'aide à la décision. L'arrivée du big data pourrait également trouver une intégration au sein des forces aériennes puisque les grands volumes de données sont censés permettre de conduire une guerre de manière plus rationnelle et scientifique. S'il est possible de mettre en doute cette vision qui ne sera peut-être pas plus capable de dépasser le brouillard de guerre qu'un esprit humain, force est de constater que le domaine de la sphère d'information tend à croitre et à prendre en importance. Ce sont d'ailleurs ces avancées technologiques qui laissent poindre la vision américaine de bataille multi domaines. La maîtrise de ces technologies donnera donc un avantage certain aux forces aériennes qui auront fait le pas d'une intégration cybernétique au sein de leurs processus. Cela ne concerne pas que les spécialistes et les *geeks* montant des opérations électroniques du fond de leur garage mais bien tous les opérateurs, du soldat au général. Plus important encore, il faut que les états-majors soient à même de comprendre les tenants et les aboutissants de ce domaine pour l'intégrer avec succès dans le plan de manœuvre général. La grande question reste de savoir si cela sera culturellement possible. L'histoire récente a déjà démontré que, parfois les terriens et les aériens, avaient de la peine à se mettre sur la même longueur d'onde alors que penser d'un *geek* qui se perdrait dans une centrale d'opérations aériennes ? En tous les cas, les potentialités technologiques pour rendre plus efficientes les armes de la troisième dimension sont là ; il ne reste plus qu'à les intégrer au plan général.

J. G.

Le site iranien de Natanz, rendu inopérant par le virus Stuxnet. Aucune infrastructure n'est désormais à l'abri d'une telle attaque.

1 Traduction libre de l'auteur.