Ces dernières années ont vu une augmentation des conflits et des tensions internationales, inter-États ou par procuration, avec l'utilisation de sociétés militaires privées richement dotées en matériels, comme on a pu le voir en Libye. La principale caractéristique de ce type d'affrontement, à l'opposé de ceux contre des groupes armés (rebelles, terroristes ou djihadistes), est la mise en œuvre d'un haut niveau technologique. Artillerie, chars de combat, aéronefs, drones, systèmes sol/air sont autant de moyens qui équipent les armées contemporaines un tant soit peu développées. À cela, s'ajoutent des moyens offensifs de guerre électronique.

La Russie a réactualisé cette pratique un peu oubliée par les Occidentaux. Ce sera une des marqueurs des différentes interventions militaires de Moscou : déployer et utiliser ce type de systèmes. La Russie est aujourd'hui imitée par les forces turques, mais d'autres nations prennent ce sujet très au sérieux comme la Chine, le Japon, Israël, la Corée du Sud, la Suède, les Émirats arabes unis, etc. Même les États-Unis montrent un regain d'intérêt très marqué pour la guerre électronique, notamment pour son volet offensif.

La prise de conscience du caractère stratégique de la maîtrise du spectre électromagnétique devient désormais générale. La ministre des Armées, Florence Parly a évoqué, lors de son audition à l'Assemblée nationale le 5 mai 2021, la nécessité de développer des capacités défensives et offensives dans le champ du cyber et de la guerre électronique[1]. Pour le moment n'est évoqué que le renforcement des capacités de renseignement électromagnétique (ROEM), mais c'est un début. Cela se traduit par les programmes[2] ARCHANGE (remplacement des C-160G d'écoute électronique), *CERES* (satellite ROEM remplaçant les satellites ELISA), ALSR (avions légers de surveillance et de renseignement en remplacement des avions loués à CAE Aviation), de systèmes interarmées de renseignement d'origine électromagnétique tactique (remplacement des moyens équipant les frégates, les avions ATL-2 et les VAB SAEC* du 54e RT), BLSR (bâtiments légers de surveillance et de renseignement devant renforcer le BEM *Dupuy-de-Lôme*) ainsi que, peut-être, de l'emport d'une charge utile ROEM sur les drones *Reaper*[3] selon le bon vouloir de Washington. Toutefois, ces annonces ne doivent pas masquer le fait que la majorité de ces programmes consiste à remplacer des capacités existantes. Ils ne représentent qu'une augmentation marginale des moyens et ne pourront pas couvrir l'ensemble des besoins.

Pourquoi ce regain d'intérêt pour la guerre électronique ?

Avec la chute de l'Union soviétique, les perspectives de conflits de haute intensité entre États s'éloignèrent et certains pensèrent même qu'ils étaient révolus. Les deux guerres du Golfe (1991 et 2003) et la guerre du Kosovo ont pourtant rappelé que cela était encore possible. Malgré tout, le rapport de force entre la coalition internationale mise en place chaque fois et l'adversaire était incroyablement déséquilibré en faveur de la première. La supériorité était écrasante dans tous les domaines, à la fois numériquement et qualitativement (entraînement, modernité du matériel, logistique…). A aucun moment lors de ces affrontements les forces occidentales n'ont été réellement menacées. Il y a bien eu quelques situations délicates mais

aucune d'elles n'aurait pu avoir un impact significatif sur l'issue des conflits. Dès la fin de la guerre du Kosovo, la France retirait du service ses derniers missiles anti-radar MARTEL, abandonnant ainsi ses ultimes capacités de suppression des systèmes sol/air adverses. Après tout, les guerres de demain se feraient en coalition aux côtés des Américains et contre des puissances secondaires, pensait-on alors.

Toutefois, depuis la crise ukrainienne et l'intervention de Moscou en Syrie, les pays occidentaux ont pu se faire une idée plus précise des capacités offensives des systèmes et des doctrines russes en a matière de guerre électronique[4]. Ils ont pu constater les effets que cela pouvait avoir sur leurs propres moyens, effets aussi variés que nombreux : brouillage des signaux GPS[5], des téléphones portables[6], des liaisons de données des drones[7] — même des plus évolués[8] —, des radars, des liaisons radios, des satellites[9], des systèmes sol/air, etc.

Les conséquences potentielles sont telles que cela a fini par inquiéter suffisamment le département américain de la Défense[10] (DoD). Selon le rapport présenté par cette administration, la Russie et la Chine font preuve d'une grande efficacité dans ce domaine. Les analystes du DoD affirment que les États-Unis risquent de perdre la maîtrise du champ de bataille s'ils ne contrôlent pas le spectre électromagnétique et constatent que les réformes dans le domaine n'ont pas apporté les résultats escomptés. Ils déclarent que la Russie été en mesure de conduire des actions *« réussies dans le monde réel contre les États-Unis et d'autres armées étrangères* ». Au fil des pages, le rapport cite des problèmes organisationnels, des matériels obsolètes, des personnels inexpérimentés du fait d'une formation inadaptée ainsi qu'un spectre électromagnétique de plus en plus chargé et donc de plus en plus complexe à exploiter. Ce document met bien en lumière la nécessité absolue de maîtriser son environnement électromagnétique avant même de penser à y être offensif. D'ailleurs, deux législateurs[11] du *House Armed Services Committee* poussent à ce que ce domaine soit mieux pris en compte et davantage centralisé. Ils évoquent même la possibilité, qu'à l'avenir, le spectre électromagnétique puisse devenir un domaine de guerre distinct, avec son propre commandement.

L'amiral Sergueï Gorchkov – commandant en chef de la marine soviétique de 1956 à 1985 – avait déclaré, pendant la Guerre froide, que « *celui qui maîtrise la totalité du spectre électromagnétique dominera le monde*« . Compte tenu de notre dépendance de plus en plus grande au spectre électromagnétique, cette affirmation n'a jamais été autant d'actualité qu'aujourd'hui. On comprend alors que la guerre électronique redevienne particulièrement à la mode. La formule a été reprise par le général Jean-Paul Siffre dans le titre de son livre *La guerre électronique – Maître des ondes, maître du monde*. (Lavauzelle, 2004).

Quelles conséquences si on ne maîtrise pas le spectre ?

Que se passerait-il si nous avions à affronter un adversaire qui exploiterait à plein le potentiel de la guerre électronique à nos dépens ?

Premièrement, cela lui donnerait accès à tous les renseignements que l'on peut extraire de l'écoute du spectre électromagnétique (sauf à ce que des mesures soient prises pour en minimiser l'emploi ou pour faire du contre renseignement : fausse utilisation du spectre, éventuellement en association avec de leurres pour fausser le renseignement que l'adversaire pourrait tirer de ses écoutes). Cela lui permettrait de connaître l'ensemble des moyens utilisés et déployés, d'en déterminer le positionnement approximatif et éventuellement nos intentions. Il connaîtrait donc parfaitement le rapport de force, les points forts et les points faibles du dispositif.

Deuxièmement, la privation de nos moyens de navigation satellitaire (GNSS) compromettrait directement la mise en œuvre de certains armements guidés (missiles, bombes, roquettes, obus). De quoi grandement compliquer le déplacement des unités (terrestres, aériennes ou navales) qui se retrouveraient sans moyens de navigation de grande précision. Il deviendrait aussi bien plus difficile de repérer et de détruire des cibles avec certitude : comment trouver, dans une ville, le bon bâtiment si on n'est pas capable d'en déterminer l'emplacement exact et alors même que l'on ne connaît pas soi-même parfaitement sa propre position ? Paradoxalement, ce sont les équipements militaires qui sont les plus vulnérables à un brouillage ou à un « *spoofing* » (usurpation de signaux pour décaler la position réelle) des signaux de navigation par satellite. Contrairement aux équipements *« grand public »*, qui utilisent et recoupent très souvent les informations de trois ou quatre systèmes GNSS différents, les militaires occidentaux n'en utilisent généralement qu'un seul. En dehors du projet P3TS[12] de l'armée de terre, qui est le premier récepteur militarisé recueillant et synchronisant à la fois les signaux de géolocalisation par satellite du GPS (États-Unis), du GLONASS (Fédération de Russie) et de GALILEO (Union européenne), rares sont les systèmes militaires reposant sur différentes sources GNSS. On imagine facilement la difficulté, pour les militaires occidentaux d'accepter de recouper leurs données de positionnement avec les constellations russes GLONASS ou chinoises BEIDOO. D'autant que le système GPS dispose d'un mode militaire crypté, accessible aux pays de l'OTAN, offrant une bien meilleure précision. Donc aujourd'hui encore, les armées occidentales se reposent essentiellement sur le GPS américain, même si le système européen GALILEO commence à être pris en compte.

Troisièmement, la privation de tout ou partie de nos moyens de communication aurait des conséquences très graves sur la conduite des opérations. Concrètement, cela signifie ne plus être capable de transmettre les ordres aux forces déployées (terrestres, navales, aériennes) mais aussi ne plus connaître la position, ni le statut des unités sur le terrain (absence de comptes rendus). En conséquence, il devient impossible de fournir un appui à une unité en difficulté. Il n'y a alors plus de coordination entre les éléments qui deviennent plus ou moins livrés à eux-mêmes. Cela implique également de ne plus recevoir les renseignements issus des forces sur le terrain ou des plateformes ISR *(Intelligence, Surveillance, Reconnaissance)*. Donc, sans renseignement à analyser, plus possible de dresser de situation tactique, c'est le brouillard qui s'installe. Le seul *« avantage »* est qu'il n'y aura plus les problématiques liées au *Big Data*. Plus besoin de l'IA pour traiter le flux de données puisqu'il n'y en aura plus ou très peu. Il est aussi probable que, dans ces circonstances, la faible quantité de données qui parviendrait soit celle que l'adversaire voudrait bien laisser passer. Il serait à craindre que ces informations soient potentiellement fausses, ou tout au moins incomplètes, afin de, non seulement de nous priver de vision tactique, mais de nous en donner une fausse image.

Quatrièmement, la privation de nos moyens d'identification comme les IFF *(Identification, Friend or Foe)* ferait qu'il ne nous serait plus possible de reconnaître avec certitude nos propres unités : risque d'autant plus grand que les communications seraient elles aussi perturbées. Potentiellement cela pourrait amener des forces alliées à s'affronter entre elles ou à abattre, par erreur, un de leurs appareils. Cela arrive déjà parfois suite à de simples pannes ou dysfonctionnements techniques ; mais dans une situation de brouillage global, les risques de tirs fratricides seraient multipliés, d'autant plus que les opérations d'aujourd'hui favorisent largement la dispersion des forces et leur mobilité.

Cinquièmement, la privation de tout ou partie de nos moyens de détection longue portée ainsi que de nos systèmes d'armes (brouillage des aéronefs, des navires, des systèmes sol/air, des radars de veille…) nous rendrait non seulement aveugles, mais aussi impuissants. Perdre ses capacités de détection, c'est perdre toute faculté d'alerte et c'est donc devoir subir la surprise stratégique ou tactique sans pouvoir réagir car nombres de systèmes d'armes seraient aussi neutralisés.

Bien entendu, il est très peu probable de devoir subir tous ces effets simultanément sur l'ensemble des forces d'un théâtre d'opération : cela demanderait à l'adversaire des moyens de guerre électronique absolument considérables. Mais cela peut tout à fait se produire ponctuellement dans certaines zones géographiques, permettant ainsi à l'ennemi de prendre l'avantage là où il le décide en paralysant les forces qui lui sont opposées. Naturellement, cette tactique de guerre électronique offensive ne peut avoir un impact significatif qu'au prix de l'utilisation de moyens technologiques conséquents. Des troupes rebelles seulement équipées d'armement individuel léger ne seront que très peu impactées car elles utilisent aussi très peu le spectre électromagnétique. C'est d'ailleurs sans doute en raison de cette pratique de la *« petite guerre »* depuis plusieurs décennies qui fait que les armées occidentales ont délaissé leurs capacités de guerre électronique.

***

La guerre électronique peut avoir une influence énorme sur le déroulement des opérations militaires. Tous les systèmes et équipements des armées modernes sont dépendants, d'une manière ou d'une autre, des radiofréquences et tous peuvent voir leur fonctionnement plus ou moins dégradé dès qu'ils en sont privés, au point de, potentiellement, neutraliser complètement la puissance militaire mise en œuvre.

Il est essentiel de surveiller le spectre, non seulement pour détecter les menaces, mais aussi pour repérer les brouillages dont on peut être victime, et cela, avant même de songer à être offensif. La majorité des menaces représentées par des forces militaires modernes porte une signature électromagnétique détectable qui représente une opportunité à exploiter.

La surveillance du spectre permet d'anticiper certains dangers comme des drones (détection des liaisons de données), des aéronefs (détection des radars ou des communications), des forces ennemies (liaison radio) etc. Cela offre aussi la possibilité de réagir rapidement face à la détection d'un brouillage pour en limiter l'impact (changement de mode opératoire) : un brouillage est aussi synonyme de la présence d'un ennemi qui vous a détecté d'une manière ou d'une autre. Après tout, les armées sont habituées à surveiller leur environnement dans le

domaine du visible, de l'Infra Rouge, du sonore, souvent aussi avec des radars ; alors pourquoi délaisser l'écoute des radiofréquences ?

En France, les unités de guerre électronique sont peu nombreuses. En conséquence, rares sont les unités militaires capables d'évoluer en ayant conscience et connaissance de leur environnement électromagnétique. Pourtant, le spectre électromagnétique est de plus en plus dense, complexe, évolutif. Le surveiller demande du temps, des personnels particulièrement bien formés et expérimentés. Au-delà même du nombre de capteurs de guerre électronique disponibles, c'est souvent la ressource en personnel qui fait le plus défaut. Dans ces conditions, il devient nécessaire de développer des capteurs moins chers, plus légers, faciles à installer, au fonctionnement plus simple, en partie automatisés afin de pouvoir les déployer dans toutes les unités et sur tout type de porteur, sans exiger d'accroître le nombre de spécialistes du domaine.

Les armées modernes qui sont amenées à évoluer dans un environnement électromagnétique dégradé voient leurs capacités tactiques grandement diminuées, d'autant plus que leur connectivité est aujourd'hui un des principaux démultiplicateurs de puissance. Comme nous ne disposons pas des armes pour reconquérir l'usage du spectre, a minima devrions-nous disposer des outils permettant de détecter les menaces dans cet espace pour nous soustraire, autant que possible, aux gênes occasionnées.

Il est vrai que la guerre électronique ne peut, à elle seule, faire gagner un conflit ou une bataille. Mais aujourd'hui, face à un adversaire technologiquement avancé, perdre l'affrontement dans le spectre électromagnétique, c'est immanquablement s'assurer la défaite dans tous les domaines.

Olivier DUJARDIN / CF2R

—

* SAEC : Station d'appui électronique de contact