La guerre électronique dans les conflits aujourd'hui

Dylan Rieutord, directeur du Pôle Armées de l'Institut d'Études de Géopolitique Appliquée, s'est entretenu avec Olivier Dujardin, chercheur associé au CF2R (Centre français de recherche sur le renseignement), responsable de la rubrique technologies et armement et consultant indépendant. Il a plus de 20 ans d'expérience dans la guerre électronique, le traitement des signaux radar et l'analyse des systèmes d'armes. Olivier Dujardin a successivement exercé des fonctions opérationnelles dans la guerre électronique, dans l'étude des systèmes de radar, de guerre électronique, l'analyse et la collecte de signaux électromagnétiques. Il a également occupé le poste d'expert technique en systèmes de recueil SIGINT.

Comment citer cet entretien :

Olivier Dujardin, « La guerre électronique dans les conflits aujourd'hui », Institut d'Études de Géopolitique Appliquée, Septembre 2021. URL : cliquer ici

---

Dylan Rieutord - Quel est l'impact concret de la guerre électronique dans un combat ?

Olivier Dujardin - Premièrement, laisser à un adversaire le monopole de la guerre électronique, c'est lui donner accès à tous les renseignements que l'on peut extraire de l'écoute du spectre électromagnétique (moyens déployés et utilisés, positionnement des forces, intentions, etc.). 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). Cela compliquerait aussi grandement le déplacement des unités (terrestres, aériennes ou navales). Il deviendrait aussi bien plus difficile de repérer et de détruire des cibles avec certitude : comment repérer dans une ville le bon bâtiment si on n'est pas capable d'en déterminer l'emplacement exact et si l'on ne connaît pas soi-même parfaitement sa propre position ?

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 unités, mais aussi ne plus connaître la position ni le statut des unités sur le terrain. Il n'y a alors plus de coordination entre les unités qui deviennent plus ou moins livrées à elles-mêmes. Cela implique également de ne plus recevoir les renseignements issus des unités ou des plateformes ISR (Intelligence, Surveillance, Reconnaissance). Sans renseignements à analyser, il n'y a plus de situation tactique et c'est le brouillard qui s'installe. Il serait aussi à craindre que les seules informations qui arrivent soient potentiellement fausses, ou tout au moins incomplètes, afin de non seulement nous priver de vision tactique, mais de nous en donner une fausse.

Quatrièmement, la privation de nos moyens d'identification comme les IFF (identification friends 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 démultipliés, 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 nombre 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'opérations : cela demanderait à l'adversaire des moyens en guerre électronique absolument considérables. Mais cela peut tout à fait se produire ponctuellement sur 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.

D.R - Le retard accumulé en Europe voire en Occident peut-il être comblé que ce soit niveau matériel ou des TTPs ? Si oui, quelles orientations par exemple?

O.D - Oui le retard pourrait être comblé. Si on prend le cas de la France, nous disposons du tissu industriel nécessaire au travers des grands groupes connus, mais il ne faut pas oublier les TPE/PME dont plusieurs peuvent apporter des solutions innovantes à plus faible coût. Nous pourrions donc disposer des moyens techniques adéquats pour peu qu'ils soient correctement définis.

Autre point, les armées françaises disposent encore de filières de formation pour les spécialistes de la guerre électronique. Nous disposons donc d'un vivier, certes restreint, mais néanmoins bel et bien existant de personnes formées et compétentes. Cette compétence au sein des armées est une richesse, car c'est un socle sur lequel on peut s'appuyer pour remonter en puissance. Il serait aussi possible de faire appel aux anciens militaires passés dans le civil, comme le font des Anglo-saxons qui savent valoriser les expériences acquises au travers de sociétés privées en contrat avec l'État.

> Bien entendu toute remontée en puissance devrait se faire sur la base d'une réflexion conceptuelle et d'expérimentations opérationnelles de façon à tester les idées. Malheureusement c'est cette réflexion de fond qui manque un peu en France.

La situation des pays occidentaux est très variable et dépend pour beaucoup des réformes engagées ces vingt dernières années. Aujourd'hui seuls les États-Unis font un réel effort pour

revenir sur le devant de la scène relativement rapidement. Si la France le décidait, elle le pourrait aussi, surtout que la guerre électronique est un domaine qui a un rapport coût/efficacité particulièrement favorable par rapport à bien d'autres. C'est surtout une question de volonté, nous avons le potentiel technique et humain.

D.R - Comment voir l'avenir de la GE en termes d'emploi et de capacités ? Quelles sont les tendances prises par les États ou les groupes non étatiques ?

O.D - On peut déjà le constater, mais le poids de la guerre électronique va croissant à mesure que les perspectives de conflits entre puissances militaires développées se précisent. Depuis l'intervention russe en Crimée, pas une seule de leurs opérations ne s'est fait sans de puissants moyens de guerre électronique et avec un certain succès. Les occidentaux ont pu être témoins, en Syrie notamment, mais aussi lors d'exercices militaires russes, que ceux-ci mettaient les moyens pour être en mesure d'attaquer toute forme d'utilisation radios fréquences (brouillage ou spoofing des signaux GPS, brouillage radar, des communications, des liaisons de données des drones, des GSM, des satellites...). Je pense que c'est une tendance lourde dont il faut tenir compte. D'ailleurs la Russie n'est plus la seule à faire des efforts dans ce domaine, on peut citer la Turquie qui a développé ses propres capacités, les États-Unis qui réinvestissent le domaine, mais on peut souligner aussi les efforts du Japon et de la Corée du Sud. On peut même parler des Emirats arabes unis qui achètent du matériel d'écoute et de brouillage.

> Pour le moment, en dehors du brouillage GPS, il ne semble pas que des groupes non étatiques se soient lancés dans ce domaine, mais quand on voit que la société militaire privée russe Wagner a mis en œuvre des systèmes antiaériens *Pantsir* en Libye, on peut se dire que ce n'est qu'une question de temps.

Toutefois, c'est une discipline qui demande un certain savoir-faire, des connaissances et un matériel difficilement accessible pour des groupes terroristes par exemple.

D.R - Comment ne pas devenir totalement dépendant et se protéger de l'émission EM ?

O.D - Pour éviter une dépendance totale au spectre électromagnétique, il faut pouvoir faire sans.

Concernant la radio ou les liaisons de données, cela passe par garder des procédures un peu oubliées et s'entraîner avec. Par exemple, il existe des procédures permettant d'identifier un aéronef ami sans contact radio ni IFF. Cela se traduit par des procédures de rendez-vous à des points précis, à des horaires précis à une vitesse et une altitude prédéfinies à l'avance voire par des manœuvres spécifiques. Cela passe aussi par une plus grande liberté laissée aux chefs sur le

terrain. En réalité tout le savoir-faire existe pour se passer autant que possible des liaisons radio fréquences, mais ce sont des procédures qui ne correspondent plus forcément au fonctionnement des états-majors habitués à être abreuvés en temps réel des informations remontées par chaque unité.

Se passer de radar passe par accepter de disposer de plus de moyens de reconnaissance qu'ils soient humains, aériens ou maritimes. Cela impose un peu plus de masse aux armées, car elles doivent alors occuper ce qu'elles ne peuvent plus surveiller à distance.

La protection contre les émissions électromagnétiques implique deux volets distincts :

- Le premier est de se protéger du brouillage et pour cela il faut d'une part contrôler le spectre électromagnétique, donc le surveiller et, d'autre part, être agile sur le spectre de façon à y échapper ;
- Le deuxième implique d'être discret sur le spectre de façon à éviter la détection. Cela peut être la mobilité des émetteurs pour éviter d'être localisé, de se cacher dans le spectre ou de limiter ses émissions et les durées de celles-ci.

Bien entendu tout cela passe par l'acceptation que l'on ne pourra pas pleinement bénéficier de l'hyper connectivité que permet la technologie. C'est un peu en contradiction avec les tendances actuelles du combat info valorisé multi domaine qui est largement mis en avant comme permettant d'obtenir une supériorité opérationnelle sur l'adversaire.

D.R - Pensez-vous que la bombe IEM qui provoquerait un black-out total et couperait ainsi toutes communications à l'échelle d'une ville relève d'un fantasme ou d'une attaque possible? Je pense personnellement que ce risque serait plus à prendre en compte sous l'aspect cyber avec des attaques informatiques ciblées.

O.D - La réponse à cette question est complexe, car cela dépend du type d'IEM dont on parle (nucléaire à vocation stratégique, non nucléaire à vocation stratégique, non nucléaire à vocation tactique...) et du type de génération (explosive ou à base de générateurs).

Sans rentrer dans les détails, il faut retenir plusieurs notions pour comprendre les différents cadres d'emplois.

D'abord les effets d'une IEM vont dépendre de la nature de la cible et de sa protection « naturelle » : un bâtiment en béton armé sera moins impacté, car le ferraillage du béton agira comme cage de Faraday, de même un char de combat sera moins impacté qu'un avion.

Ensuite, tout système antennaire est une porte d'entrée naturelle aux IEM et donc, dans certains cas, cela peut pénétrer certaines structures, à priori protégées, *via* ce canal. Mais là encore l'impact doit être étudié pratiquement au cas par cas. Par exemple une IEM peut griller les

communications d'un char, mais ne le mettra pas hors de combat en revanche la même IEM peut descendre un aéronef, immobiliser un camion ou une voiture ou priver un soldat de sa radio, des jumelles de vision nocturne, de son GPS, etc.

Enfin, il faut aussi garder à l'esprit que la densité de champs électromagnétique d'une IEM diminue au rythme du carré de la distance, car l'absorption atmosphérique est importante et la focalisation du faisceau (pour les armes à générateur) est globalement faible (le rayonnement est isotrope pour les IEM explosives). En clair c'est une arme à courte distance. Si on doit la comparer avec des armes légères, une arme à générateur est équivalente à un fusil à pompe, la génération doit donc être proche de la cible. En comparaison, le Laser peut, lui, être comparé à un fusil de précision.

Pour répondre à la question, il est possible de créer un blackout total sur une ville avec une IEM, mais cela demande une bombe de très forte puissance voire une arme nucléaire. Ce ne serait pas forcément l'approche la plus pertinente. Par contre cela peut être pertinent pour dégrader les capacités de combats des forces adverses qui sont au contact.

C'est cette difficulté à appréhender tous ces aspects qui explique que ces armes sont aujourd'hui encore peu utilisées, c'est ce que j'avais développé dans un article l'année dernière : https://cf2r.org/rta/armes-a-impulsion-electromagnetique-pourquoi-sont-elles-encore-tres-peu-utilisees

D.R - Vous avez parlé de brouillage, d'écoute, de localisation, de communication, quid des opérations de déception ou de ruse sur le spectre EM ? Avez-vous des exemples de tactiques célèbres ou moins connues ?

O.D - Oui cela existe. Par exemple, les Russes peuvent utiliser le système ECMC-125 qui est un émulateur de radar de conduite de tir du S-300. Il sert, associé à des leurres gonflables, à dévier de leur trajectoire les missiles antiradars. Il peut aussi servir à créer de fausses stations sol/air de façon à faire croire que la défense anti aérienne est plus dense qu'elle ne l'est réellement ou pour diluer les vraies batteries avec des fausses. Je n'ai pas connaissance de systèmes équivalents en occident.

Le cas le plus ancien de déception sur le spectre EM que je connaisse remonte à 1917 lorsque les Zeppelins allemands utilisaient les émetteurs de la tour Eiffel pour se guider vers Paris. Les Français ont eu alors l'idée, lorsqu'ils détectaient les communications d'un Zeppelin, de couper les émissions de la tour Eiffel au profit d'émetteurs situés loin de Paris et ainsi les Zeppelins s'égaraient et loupaient la capitale.

D.R - **Comment réussir l'allocation intelligente de la ressource fréquence dans les villes où les combats s'intensifieront et là où le nombre de capteurs (civils comme militaires) va exploser au travers de la robotique, de l'IoT et des communications ? Quels avantages/inconvénients**

soulèverait la collusion des gammes de fréquences civiles et militaires ?

O.D - Les gammes de fréquences utilisées par les applications civiles sont parfaitement connues et délimitées. Les militaires peuvent utiliser des plages de fréquences bien plus larges, mais également les plages civiles. La conséquence est que le spectre est de plus en plus chargé. Cela présente l'inconvénient que le risque d'interférence est bien plus important même si les émetteurs militaires opérant sur les gammes civiles sont généralement plus puissants. Il peut aussi être plus compliqué de trouver suffisamment d'espace fréquentiel libre pour toutes les applications. Néanmoins, un spectre très chargé présente l'avantage qu'il est bien plus facile de se cacher dedans. La surveillance du spectre devient de plus en plus complexe à mesure que le nombre d'émetteurs croît.

Dans tous les cas, que ce soit pour allouer les fréquences, éviter les interférences ou se cacher dans le spectre, cela implique de le maitriser et donc de le surveiller en permanence. Malheureusement, compte tenu du peu d'unités spécialisées et du peu de matériel disponible pour cette tâche, c'est rarement le cas en pratique.

secretariat@institut-ega.org

N°SIRET - 849 769 906 00025