Contribution (Liberte-algerie.com) (*)

L’ordre de bataille électronique est déjà engagé face à l’impérialisme

©Liberte-algerie.com

Le titre de cet article n’est pas du tout pamphlétaire, la guerre électronique et plus précisément l’ordre de bataille électronique est bel et bien engagé et fait rage en Syrie entre la Russie d’une part et l’OTAN et les américains d’autre part (les forces impérialistes).

L’entrée en lice de l’armée russe sur le front syrien a suscité l’engouement de toute la presse internationale pour percer et comprendre les mystères de ces équipements de guerre électronique qui ont permis aux russes d’imposer aux occidentaux une zone d’exclusion aérienne. C’est à ces interrogations que tente de répondre cet article.

A la gestion classique d’opérations militaires de champs de bataille apprises dans toutes les académies militaires, au cours de ces dernières décennies est venu s’ajouter l'importance d'un nouveau système d'information entièrement automatisé, moderne, hypersophistiqué, ayant à son actif des succès foudroyants, durant les récentes guerres de Serbie ,d’Irak et de Syrie. Ce système est appelé C4I. Il est nécessaire pour que les opérations engagées soient réussies, de disposer de la bonne information, l’homme n’a pas les moyens cognitifs de traiter des millions d’informations dans un champ de bataille pour réagir vite avant l’ennemi, où le temps de traitement et de réaction sont presque confondus, de l’ordre du milliardième de seconde (détection et réponse aux menaces sous les feux de la bataille). Pour soutenir toutes les phases de la gestion et de

l'exploitation (acquisition, le stockage, la diffusion, la récupération et l'exploitation) des informations d'une manière rentable et sécurisée, il faut que le commandement puisse gérer et contrôler automatiquement tous les résultats de tous les scénarios réels de champs de guerre (aérienne, terrestre, navale et électromagnétique).

Pour décider de l'issue de la bataille, la possession et la maîtrise de l'information, permet d'agir avec une grande efficacité. Par exemple :

Le tir réussi contre une cible dont les coordonnées ont été fournies par les systèmes d'informations.

Un soldat dans le désert ou dans la montagne, ratissait à l'aveugle le terrain juste il y a quelques années, peut avoir maintenant dans son écran d'ordinateur portable des informations sur le champ de bataille locale : la position de groupes isolés, la position de l'attroupement des forces ennemies et les cibles matériels à détruire, même s'il ne dispose pas des capteurs et senseurs adéquats, pour déterminer le temps, l'espace et le nombre de renforts pour engager l'opération.

Un navire au milieu de l'océan peut recevoir via la communication par satellite la situation environnante complète (une image très large de la zone (400 kms de diamètre)) de la confrontation navale, même si l'ennemi utilise un mode complet de navigation silencieux et sans signal radar (radar éteint).

Les puissances impérialistes, jusqu'à récemment, la guerre de Syrie avaient une suprématie aérienne et électromagnétique totale grâce au système automatisé C4ISR (Command, Control, Communications, Computer, Intelligence, Surveillance et Reconnaissance). La puissance des airs, est la principale composante d'une guerre dite de théâtre ou conventionnelle. Elle consiste à détruire et supprimer totalement les défenses aériennes (radars, missiles, artillerie anti-aérienne) et empêcher que les forces aériennes adverses puissent décoller, voir les neutraliser (Agressions impérialistes contre l'Irak et la Lybie). Mais l'issue finale de la bataille ne se fera que si on marche à pieds.

Une grande surprise (reprise par toute la presse spécialisée militaire dans le monde) attendait les connaisseurs et spécialistes de la guerre électronique qui ne s'imaginaient pas que les russes puissent reproduire en Syrie le scénario passé de la mer noire du printemps 2014 du Su-24 qui n'avait embarqué ni missile ni bombe, armé seulement du boitier de guerre électronique Khibiny qui a mis en déroute le destroyer américain USS Donald Cook malgré que celui-ci armé jusqu'aux dents (96 missiles de croisière Tomahwak et 50 missiles anti-aériens) est devenu subitement sourd et aveugle.

Le système Khibiny russe a débranché le radar, les commandes de combat et le système de transmission des données du système Aegis de l'US Navy comme on éteint une télévision. Sauf que cette fois-ci en Syrie, les russes ont reproduit le même scénario dans une ampleur gigantesque, sur un rayon de plus de 300 km, d'avoir réussi à fermer l'accès à l'espace électromagnétique du territoire syrien aux puissances impérialistes et à leurs alliés terroristes (Access Denied).

Je rappelle que le système AEGIS (C4ISR) américain, réunit les moyens de défense antimissiles de tous les navires qui en sont équipés pour former un réseau commun permettant d'identifier, de suivre et d'attaquer des centaines de cibles à la fois.

De l'aveu même du commandant militaire de L'OTAN le général Philip Breedlove le 23 octobre dernier qui a reconnu publiquement que les américains et leurs alliés viennent de subir la pire des humiliations de se retrouver exclus de la zone aérienne syrienne. La Russie a créé une zone d'exclusion, impénétrable pour tous moyens de l'OTAN (Anti-Access/ Area Denial- A2/AD bubble).

Ce qui est nouveau cette fois, dans les opérations de guerre en Syrie, à haute intensité létale,'' hard kill '', la suprématie totale du système d'informations russes C4ISR a altéré de façon drastique celui de l'alliance

atlantique et des américains. Pour atteindre cet objectif, dans la zone contrôlée, les russes ont réduis fortement le système d'information adverse afin qu'ils ne puissent plus disposer de moyens de communication SIGINT (voir explication ci-dessous).

Le premier résultat de l'intervention russe en Syrie ne tarda pas à venir : les américains et l'OTAN sont fixés définitivement de l'incapacité de leurs logiciels sophistiqués C4ISR (dépenses cumulées de plus de 189 milliards de dollars en l'espace d'une décennie qui n'ont servies à rien malgré le concours de toutes les compagnies occidentales et israéliennes de fabrications d'équipements et de logiciels de guerre électronique) à faire face aux technologies russes. Les russes viennent de démontrer magistralement que l'OTAN serait une proie facile pour Moscou.

Comment ?

Par des attaques électroniques massives, parfaitement organisées au moyen de systèmes ESM-ELINT (explications plus loin, ci-dessous) couplés au complexe automatisé C4I (Command, control, Communication et Computer et intelligence) , système, qui consiste à empêcher l'adversaire d'utiliser le spectre électromagnétique, spectre qui regroupe l'ensemble de toutes les ondes électromagnétiques en fonction de leur longueur d'onde et de leur fréquence : il s'agit donc pour l'essentiel de mesures de brouillage de ses émissions et de mesures de leurrage ou d'intrusion.

La guerre conventionnelle moderne repose sur le complexe automatisé « C4I », Command (piloter, maitriser), Control, Communication, computer (ordinateurs et informatique) et intelligence (renseignements : SIGINT, HUMINT, MASINT, IMINT et tout les mult-INT) et une force aérospatiale (drones et satellites). L'expérience syrienne démontre que le système russe est le plus performant, mais ses principes de base et son modus operandi restent entourés de mystère.

Dans le système automatisé C4ISR, tous les équipements, satellitaires, aériens, terrestres et navals et les combattants qui participent dans un champ de bataille travaillent en réseau et sont reliés les uns et les autres par des communications permanentes qui permettent aux états majors de commander des batailles en temps réel pour détruire de façon intensive un maximum de cibles en immobilisant et en gelant tous mouvements de l'ennemi pour qu'il ne puisse pas se déplacer afin de pouvoir l'achever et l'anéantir totalement sur ses positions fixes révélées, tout en suivant l'état des stocks opérationnels et du confort des troupes engagées (munitions, carburant, alimentation ultra énergique et poly vitaminés, latrines, prise en charge rapide des blessés, de la fatigue, du confort pour revigorer le moral des combattants etc..). C'est tout le système nerveux ESM-ELINT couplé au C4I de l'Otan et des américains qui est actuellement brouillé par les russes en Syrie et dans une partie de la Turquie. Il faut ajouter que le système automatisé C4I russe réunit les dernières générations de microprocesseurs et de matériel de communication par satellite, intégrant des capteurs de détection et de guidage. Ils disposent en outre, d'installations de mémoire et de serveurs propres avec des puissances de calcul et de traitement de dernière génération sont sécurisés par cryptage numérique dans toute la gamme des fréquences, rendant impossible tout brouillage. Le C4I réparti automatiquement les cibles détectés par structure de reconnaissance vers chaque système (3 systèmes C4ISR russes opèrent déjà en Syrie, réparties en fonction du rayon d'action, par zone opérationnelle) de frappe terrestre russe et syrien (pièce d'artillerie, char, missile), ou vers ceux placés à bord de navires ou d'avions. Le C4I permet aussi la transmission et la réception audio et vidéo avec un équipement sans fil, dans des conditions sécurisées, une grande quantité de données à haut débit telles que la voix et des données numériques, en présence de brouillage. Ses éléments disposent d'installations de mémoire, accèdent à leurs propres serveurs gérés par de puissants processeurs de dernière génération, et couvrent le spectre entier des fréquences, et sont sécurisés par un cryptage numérique.

Il faut ajouter que le système modulaire C4I permet la création de réseaux tactiques de communication par l'intégration dans une plateforme telle qu'un véhicule militaire en mouvement. Il permet l'affichage et la mise à jour automatiquement de la situation tactique sur consoles avec des cartes numériques, la gestion des

contrôles, les rapports de combats, et la situation de la logistique et de surveiller l'état de préparation et de fonctionnement des systèmes d'armement. Le système C4I permet, également, d'assurer la collecte, la transmission par satellite et l'analyse des Informations au format standard de l'OTAN en temps réel grâce à des capteurs placés aux avant-postes en première ligne, et grâce aux systèmes AGS (Alliance Ground Surveillance), destinés à l'observation / suivi électronique du terrain par des moyens satellitaires et de drones performants. Toutes les informations sont dirigées vers le poste de commandement mobile au niveau de la compagnie, du bataillon ou de la brigade. Ainsi, il est possible de connaître la situation sur le plan tactique, la gestion du champ de bataille, de faciliter la prise de décision par le commandement.

Les russes savaient que les systèmes de surveillance aérienne et spatiale de l'OTAN étaient en mesure de contrôler toute l'activité des avions militaires russes basés en Syrie. Grâce aux avions de reconnaissance américains RC135, aux avions britanniques Sentinel R1, aux avions-radars AWACS et aux drones Predator, déployés sur le lime syrien, il est possible d'intercepter : le trafic radio sur les réseaux russes, le nombre et le types d'avions, les trajectoires de vol, le type d'arme utilisé, les objectifs ciblés chez les terroristes et leur emplacement. Il faut savoir que dans ces guerres que l'Otan et les américains fomentent en Irak, Syrie et prochainement en Algérie, se ressemblent toutes, les terroristes seront armés, financés et soutenus par les États-Unis et leurs alliés et que ces mêmes terroristes seront toujours avertis à temps pour chaque opération grâce à des équipements satellitaires sophistiqués qui leur seront fournis (il ne faut jamais sous estimer l'ennemi, quel qu'il soit). Nous n'avons pas d'autres solutions, que de renforcer notre alliance stratégique avec la Russie et la Chine.

Le brouillage rend inexploitable les émissions de l'adversaire ; le leurrage et l'intrusion lui donne de fausses indications ou de fausses pistes (Deception). L'ensemble de ses moyens étaient autrefois appelés contre-mesures électroniques (CME), en anglais ECM pour Electronic Counter Measures. L'attaque électronique inclut également l'emploi d'armes à énergie dirigée, destinées à détruire les systèmes électroniques adverses ou pour aveugler par laser (pilote d'avion, de combat, infanterie, chars,…). L'attaque électronique implique l'utilisation de moyens actifs, donc indiscrets.

Comment les avions russes sont ils arrivés en Syrie sans que personne ne s'en aperçoive ?

Primo, les russes ont su bâtir en Syrie un système redoutable automatisé de collecte et de traitement de l'information, maitrise, contrôle, communications, puissants moyens de calcul (ordinateurs) , renseignements et interopérabilité. Ce système permet l'identification des cibles de bombardement et leur répartition parmi les différents types d'avions. Le modus opérandi des russes est totalement ignoré par les américains et leurs alliés, ce qui fait qu'ils sont dans l'incapacité totale de déclencher de contre-mesures (ECM) efficaces contre les russes en Syrie. Un autre fait important à révéler, chez les militaires russes, il n'existe pas de traitre parmi eux pour livrer les protocoles datas aux impérialistes, c'est spécifique à l'âme russe comme l'a si bien décrit Tolstoï dans ses deux grands romans Guerre et Paix et Anna Karénine.

C'est grâce à un équipement russe de guerre électronique de dernière génération appelé Krasukha-4 disposé sur la base aérienne de Hmeymim en Syrie, que les russes ont créé un bouclier d'invisibilité pour les objets dans les airs et le sol avec un rayon allant de 300 à 500 km. Le Krasukha-4 est en mesure « d'aveugler » les radars de détection et de guidage des missiles anti-aériens MIM-104 Patriot situés sur la frontière turque, et également les radars des avions de chasse F-16C turcs décollant de la base incerlik.

Sous la protection des Krasukha-4 et d'autres systèmes de brouillage (Rytchag, Atvobaza, Krassoukha, President-S, Rtout) qui génèrent des contre-mesures y compris dans le spectre visible, infrarouge ou laser, contre les moyens optoélectroniques de surveillance aérienne et satellitaire (IMINT) des puissances impérialistes. Des dizaines d'avions russes n'ont pas été détectés par l'OTAN durant leur vol et leur atterrissage en Syrie, mais seulement quelques jours après qu'ils soient arrivés sur la base aérienne de Hmeymim.

A la suite des mesures de guerre électronique appliquées par les Russes, les terroristes islamistes ‘’modérés’’ qui étaient informés par les Etats-Unis depuis 2012, sur tous les mouvements de l’armée syrienne, n’ont plus de données sur la concentration en secret des troupes syriennes sur les axes, Lattaquié-Idlab, Lattaquié-Hama et Lattaquié-Homs. Cela a permis à l’armée syrienne, appuyée par des bombardiers russes, de déclencher des actions offensives avec des blindés pour reprendre aux terroristes le contrôle du segment Hama-Homs de l’autoroute M5 qui relie Damas à Alep.

Le Krasukha-4 russe est un équipement à bande large mobile, monté sur le châssis 8X8 de type BAZ-6910-022, qui brouille les radars de surveillance des satellites militaires, les radars au sol et aériens de type AWACS et ceux montés sur des drones. Le Krasukha-4 est le seul système au monde capable de brouiller les satellites-espions américains de la classe Lacross/Onys. Ces satellites évoluent sur orbite basse et sont équipés de SAR (Synthétic Aperture Radar) qui leur permet de pénétrer la couche de nuages ainsi que le sol ou les murs des bâtiments, avec une résolution de 20 cm.

En sus du Krasukha-4, les avions russes Su-24, Su-25 Su-34 sont équipés de systèmes de brouillage SAP-518 et SPS-171 et les hélicoptères Mi-8 AMTSH avec des Rytchag-AV à cela s’ajoute le navire Priazovye spécialisé dans le brouillage et la collecte des informations de type Elint et Comint (interception de tous les réseaux de communications).

Les russes viennent de démontrer magistralement qu’ils connaissent parfaitement tout sur les américains et l’OTAN et que ces derniers ne connaissent rien sur les russes, c'est-à-dire les russes sont informés et ont décrypté tous les protocoles datas des communications discursives (COMINT) et non discursives (ELINT, missiles, radars, aéronefs etc…) utilisés par forces impérialistes. Redoutables avancées. Voir Annexe EW B1.

Je vais développer maintenant les rudiments indispensables, les principes de bases et élémentaires, couvrants les différents aspects de la guerre électronique – contremesures électroniques (ECM), mesures de protection électroniques (EPM) et mesures de support de la guerre électronique (ESM) – que nous prolongerons avec la combinaison avec d’autres capacités ou mesures électromagnétiques qui rendent possibles de nouvelles activités basées sur les effets.

Par exemple, l’ESM, l’EPM et l’ECM pourraient avoir un rôle dans la défense électronique d’un vecteur aérien ou d’une force terrestre à l’encontre respectivement des missiles anti aérien portables (MANPADS), les missiles à fréquence radio ou les engins commandés à distance. Ces principes et leurs opus operandi, sur lesquels est bâtie la guerre électronique, je vais les développer patiemment et pédagogiquement pas à pas.

L’impérieuse nécessité d’étudier le système d’arme de l’ennemi est vitale pour les forces militaires engagées. Commençons par un petit et basique exercice d’application que connaissent très bien nos ‘’guerriers électroniciens’’ quand ils seront confrontés à une attaque massive de missiles hostiles. Toujours sur leur garde, ils agissent intelligemment, avant d'envisager une action contre un système d'arme de missile (nos guerriers seront la '' victime '' du blocage de fréquence par brouillage par la plateforme ennemi), ils savent comment le système d'arme de l’adversaire (missile en général) fonctionne, les principes sur lesquels il se fonde, ses problèmes et ses limites. C’est précisément en amplifiant les problèmes de capteurs de systèmes d'armes adverses que les forces de l'ennemi peuvent être affaiblies, c’est ce qu’apprend basiquement tout bon guerrier électronicien motivé ayant un excellent niveau Bac Mathématique + 3. Une fois que les problèmes sont connus, il est plus facile de neutraliser le système ennemi. Ce ci dit, tout guerrier radariste électronicien est entrainé à le faire. Nonobstant ceci, il faut aussi une sérieuse formation politique de nos ‘’guerriers électroniciens’’.

Plus concrètement,

Par exemple, si on sait que le radar de l’adversaire est utilisé pour donner une précision de repérage angulaire d'un milliradian d’angle solide (mrad, angle solide, notion très confuse en discutant avec beaucoup de

radaristes étrangers), et que c’est une exigence absolue pour la performance d'un système d'artillerie (ou missile), il est inutile d’insister pour empêcher, ou de lancer une poursuite par notre radar afin de parvenir à bloquer la fréquence de leur radar ou système d’arme sur le notre, '' break lock '' en anglais.

Une perturbation par ECM introduisant une erreur de 10 mrad suffira à réduire l'efficacité du système d'arme de manière satisfaisante.

Encore une fois, si l'on sait qu'un radar de recherche garantit une protection valable, c’est à dire qu’il peut détecter des cibles à leur portée maximale, l'utilisation des contre-mesures capables de réduire la plage de détection de moitié suffit d'indiquer que l'objectif de défense électronique a été au moins partiellement atteint.

Nous allons essayer, pas à pas, d’identifier les principes de fonctionnement de ces systèmes d’armes dont les enjeux dépendant de la performance des équipements de guerre électronique. Une armée classique s’appuie en particulier sur les systèmes d'armes suivantes:

C3I systèmes fixes ou mobiles (Commande, contrôle et communication)

SSM Systems (Surface-to-Surface Missile, missile sol-sol)

Long, Medium, and short range artillery systems (Systèmes d’artillerie à courte, moyenne et longue portée)

Search and acquisition radar systems to detect the ground attack aircraft (radars d’acquisition et de recherché pour détecter une offensive aérienne au sol)

SAM Systems (Surface-to-Air Missile, Missile sol-air)

AAA (Anti-Aircraft-Artillery, artillerie anti-aérienne))

Antimortar Radar and WLRs (radars localisateurs au sol de mortiers ou d’armes)

Armored vehicles (Véhicules blindés)

Helicopters whit wire-or-infrared-guided missiles (Hélicoptères dotés des missiles guidés par pointage ou à guidage infrarouge)

Battlefield surveillance systems (système de surveillance des champs de bataille).

Toutes les opérations qui impliquent les équipements listés ci-dessus, sont conduites en deux phases, la première est la détection, puis vient la seconde phase, l’intervention dans laquelle il faut décider, s’il faut utiliser des missiles ou d’autres armes, telle l’artillerie anti-aérienne.

En conséquence, les principaux systèmes utilisés par les forces armées contre lesquels une protection est nécessaire sont les suivants :

Les systèmes de recherche de cibles via les Radars
Les systèmes de missiles
Systèmes d’artillerie

Le fonctionnement de tous ces systèmes est fondé sur l'utilisation de capteurs électroniques.

Il a été largement démontré que les fréquences de ces capteurs défensifs peuvent être bloquées par les capteurs des missiles offensifs qui visent à détruire ces défenses.

Du concept des missions des défenses et des équipements électroniques qui leurs sont associés ainsi que leur

développement face aux nouvelles parades, sans cesse changeantes, surgit une seule variable de jeu, à savoir, le blocage des fréquences des capteurs défensifs.

Evidemment après, suivront tous les enjeux qui lui sont associés, et notamment, tout ce qui tournent autour des conséquences de cette fonction offensive de blocage des fréquences des capteurs défensifs.

Afin de mieux comprendre la manière dont ce blocage interfère avec les systèmes d'armes, il est nécessaire d'examiner plus en détail la façon dont les systèmes d'armes eux-mêmes sont structurés et comment ils fonctionnent.

Il faut pointer une donnée importante, à savoir la performance d'un système de défense aérienne dépend des capacités de la recherche radar à longue portée qui lui est associée.

Il faut ajouter, qu'un dispositif électronique conçu pour bloquer un système de détection ne peut interférer avec le capteur radar et son traitement du signal, que si les traitements de données qui a suivi peuvent avoir lieu dans les centres de commandement et de contrôle bien protégés et situés à des distances éloignées.

Pour rappel, un système de missiles se compose généralement de:

Un radar de recherche de moyenne portée (radar d'acquisition).

un certain nombre de radars de poursuite, chaque cible poursuivie au moyen du radar nous fournira des données de guidage du missile (il y a des radars qui peuvent poursuivre plusieurs dizaines de cibles à la fois).
un certain nombre de lanceurs de missiles.

Un missile peut être guidée exclusivement par les commandes du radar de poursuite (Fonction :Missile Command) ou il peut être lancé sur la base des données fournies par le radar de poursuite, une fois l'acquisition de ces signaux-donnés faites, le missile sera autoguidé jusqu'à sa cible (homing). Il y a trois systèmes d'autoguidage (homing) :

-Actif, si le missile est munie d'un capteur (la tête chercheuse comprenant un petit radar de poursuite).

-Semi-actif, si la source d'énergie est une source lumineuse rayonnée par le missile et la tête chercheuse est un radar de poursuite qui reçoit à son tour un rayonnement réfléchi par la cible.

-Passive, si le missile possède une tête chercheuse qui ne nécessite pas d'émetteur mais détecte l'énergie rayonnée par la cible dans l'infrarouge, l'ultraviolet ou le spectre de micro-ondes.

Les radars de poursuite, cherchent, détectent, acquièrent, et suivent une cible identifiée, fournissent toutes ses données à un ordinateur qui calcule avec précision le point d'interception que l'arme ou le missile vont cibler.

Pour résumer, il ressort de cet examen que tous les systèmes d'armes que nous avons examinés emploient les capteurs suivants, qui pourraient être la victime de systèmes de brouillage électronique:

Search radar (radar de recherche)
Tracking radar (radar de poursuite)
Radio-frequency seeker (systèmes de recherche en Radiofréquence)
Electro-optic search systems (systèmes de recherche électro-optique)
Infrared seeker (Autodirecteur et recherche des signaux Infrarouge)

L'analyse et l'étude des principes de fonctionnement des capteurs que nous allons présenter, nous révèlent les

faiblesses qui leurs sont inhérentes et les possibilités offertes à identifier les domaines où ils peuvent interférer les uns aux autres (offensif et défensif).

Tout ce ci pour montrer à quel point la perturbation d'un capteur est usuellement exploité pour la défense électronique.

Nous analyserons, comment les systèmes de missile opèrent. Dans une guerre, Les forces armées de défense électromagnétique se coordonnent entre eux par l'utilisation extensive de systèmes de communications qui peuvent néanmoins être brouillés ou leurrés. Ces systèmes, nous allons les examiner brièvement.

L'objectif de la défense électronique

Sur un plan militaire, la classification des capacités des défenses ou des attaques seront répertoriées, sur la base de leur forte propension destructrice ou à tuer (« « hard kill »). Nous allons examiner les systèmes de défense électronique, leurs fonctions et applications militaires, et comment en interférant avec un système offensif, ils peuvent neutraliser un ennemi de façon non létale.

L'organisation de la défense électronique.

Il convient de rappeler que l'objectif ultime de la défense électronique est de réduire l'efficience des systèmes ennemis d'armes offensives dont le fonctionnement est bâti essentiellement sur des dispositifs de détection électronique. Pour atteindre ce but, les mesures suivantes sont nécessaires:

la connaissance des dispositifs électroniques de l'ennemi. Ceci est obtenu par le suivi et l'étude des signaux qu'ils émettent (renseignement électronique (SIGINT)) par des équipements spécifiques qui doivent être en notre possession. (que je détaillerai plus tard).

La connaissance tactique, opérationnel et le fonctionnement des dispositifs de l'ennemi, savoir comment ils sont répartis ou distribués dans l'espace et les plateformes, sur une zone, ou autour d'une plate-forme, sensés les protéger des sources électromagnétiques hostiles (ordre de bataille électronique (EOB)). Ces informations sont vitales pour deux impératifs à la fois, uno pour la défense ou l'autoprotection mutuelle des plateformes et secundo pour dresser la parade nécessaire à une attaque électronique destinée à supprimer nos défenses aériennes (SEAD).

Les nouvelles générations d'équipements de contre-mesures électroniques (ECM)—brouillage, leurrage, tromperie--, ont pour but de réduire au maximum les capacités opérationnelles des appareils ennemis, y compris les radars de recherche, les radars d'acquisition, de poursuite et de suivi, les systèmes à infrarouges, les systèmes laser, et les systèmes de communication.

Pour adapter un équipement de contre-contre-mesure électroniques (CCME), dans le but de réduire ou d'éliminer une interférence ou perturbation provoquée intentionnellement par les (ECM), il est nécessaire d'incorporer des filtres d'ondes et des dispositifs spéciaux dans nos équipements.

Les systèmes de défense électronique et leurs objectifs opérationnels.

La défense électronique en général est définie et priorisée en fonction de son positionnement dans le tableau de l'organisation de guerre électronique inhérent à chaque armée. Il convient de rappeler qu'un système de défense électronique peut consister en une panoplie d'équipements non redondants de l'équipement que nous allons décrire ci –dessous. Par exemple, il est possible d'avoir deux mesures distinctes de support électronique (ESM) et (ECM), ou un système intégré, lorsque les deux fonctions sont exécutées ensemble.

Signal intelligence (SIGINT).

La mission des systèmes de SIGINT, est l'acquisition autant que possible des données sur les émissions électromagnétiques d'un ennemi potentiel ou d'un ami. Ils peuvent être classés en renseignement électronique (ELINT), systèmes qui collectent des données radar d'émission ; Et de communication (COMINT), systèmes qui collectent des données de communication de l'ennemi.

Leur fonction est essentiellement stratégique; La mission SIGINT est une activité permanente, poursuivie sans relâche par des gros avions porteurs bourrés d'électronique dans l'espace aérien international limitrophe à l'espace de l'ennemi, de l'adversaire et même d'un ami (l'ami d'aujourd'hui peut-être l'ennemi de demain), tout doit concourir pour réussir à aboutir à identifier les procédures opérationnelles de guerre électronique d'un ennemi potentiel. C'est fondamental, pour rendre les contremesures performantes et réussies.

Electronic Intelligence (ELINT)

La mission principale d'un système ELINT est d'intercepter et analyser, à des fins stratégiques, tout le rayonnement électromagnétique généré par des plateformes d'un pays potentiellement hostile ou ami.

Cet équipement doit être en mesure de définir les caractéristiques, la dépendance en temps, et l'emplacement des émissions électroniques hostiles. Il devrait également être en mesure d'analyser les signaux électroniques de l'ennemi, à la fois, en temps et en fréquence, et d'associer avec ces deux variables, un numéro de série de l'équipement de l'ennemi (c'est à dire, ''empreintes digitales'' ou signature radar), parfois même dans une relation one-to-one, ce qui rend possible de suivre le mouvement de l'équipement.

Les systèmes peuvent être aéroportés par des sondes spatiales dans le scénario électronique d'un pays potentiellement hostile. Ils peuvent aussi être d'origine terrestre, situé sur les montagnes, des sites suffisamment élevées et sur des promontoires (les plus hauts cimes côtiers, telle Lalla Khedidja, le Chelia, Murdjadjo et Tessala) ou des détroits, pour le contrôle du trafic maritime (Beni Saf , Ghazaout , proches du détroit de Gibraltar).

Les données recueillies sont généralement transmises à un centre d'analyse, sont convenablement codées, mémorisées dans une base de données, et sont mis en relation et corrélées avec les informations recueillies par d'autres dispositifs, par d'autres corps d'Etats ou amis, et à différents moments.

En quelques mots, l'objectif principal d'un système ELINT, c'est d'intercepter et analyser, à des fins stratégiques, tout le rayonnement électromagnétique généré dans un pays potentiellement ennemi ou ami.

Toutes ces informations, seront traitées conformément aux critères opérationnels établis par les organisations militaires, et utilisées pour construire des fichiers spéciaux dans lesquels toutes les émissions et d'autres caractéristiques de l'équipement ennemi seront archivés dans des fiches (bibliothèques des signaux ou librairies). Ces fichiers d'informations seront compilés pour être chargés dans la mémoire des équipements de défense électronique (terrestre, aérien et naval) pour être utilisés principalement à la détection de signaux de l'ennemi. Première importante conséquence, l'efficience des contre-mesures de la défense électronique se trouvera améliorée à 90% et assurera en conséquence une meilleure fiabilité des radars d'alerte embarqués (RWR) sur les avions de combats ou de transports.

Communication Intelligence (COMINT)

Ces systèmes sont semblables aux précédentes, mais leur tâche est l'interception et l'analyse des émissions de télécommunication et l'identification des réseaux de communication concernés.

Electronic Support Measures- Mesure de soutien électronique (ESM).

Le but d'un système ESM est de détecter la présence de plates-formes ennemies en interceptant leurs émissions électromagnétiques. Le terme désigne également tout l'appareillage qui sert à cette écoute et à la

classification des sources émettrices.

L'objectif principal de ce type de classe d'équipement est l'interception tactique. Les systèmes les plus simples sont ceux dont la principale fonction est de détecter la présence d'émetteurs déjà connus par comparaison avec des signaux interceptés avec des données électromagnétiques préalablement stockées. Ils sont appelés récepteurs d'alerte radar (RWR).

Cet équipement ESM est en constante évolution, grâce à une nouvelle technologie électronique, une mathématique (théorie du russe Arnold), et une informatique (intelligence artificielle alliée aux ultra-processeurs les plus récents (technologie de l'état solide)) très poussée, peut reconstruire par lui-même et simuler des scénarios électromagnétiques très complexes, y compris les émetteurs inconnus jamais ''vus'' auparavant, dans des temps de l'ordre de la nanoseconde voir picoseconde.

L'équipement ESM est sophistiqué et incontournable pour détecter les plates-formes ennemies engagées dans une attaque SEAD. C'est par l'intermédiaire de ce panel d'équipements nécessaires (ESM) mais pas suffisants (entre autres) que les puissances impérialistes veulent nous imposer une zone d'exclusion aérienne.

Les équipements ESM, leurs caractéristiques présentent 2 versions de sophistication, l'une moyenne et l'autre élevée. Leur tâche principale est de reconstruire presque en temps réel, un scénario électromagnétique, qui peut être très complexe et jusqu'alors inconnu, à partir de l'interception de la multitude de signaux qui se pressent sur son antenne. Habituellement, le ''trafic'' total se compose d'impulsions et des signaux d'ondes continues. Les Impulsions sont souvent très denses (en millions d'impulsions par seconde), sont dispersés sur des largeurs de bande de fréquence de quelques centaines de mégahertz à quelques dizaines de gigahertz, c'est-à-dire à quelques millimètres de longueur d'onde. L'équipement ESM utilise et crée diverses formes d'ondes, définit des scénarios électromagnétiques variés, au but de contre-attaquer, en jouant sur les modulations d'impulsions, selon un nombre d'itérations de dimensions non entières (fractales) approchant la résolution désirée pour engager la contre attaque ou l'attaque électronique.

L'objectif principal d'un tel système est de donner une image réel de l'environnement consistant à reconstituer un scénario électromagnétique, parfaitement identifiable à la fois par nos systèmes de défense par exemple, -- en découvrant la présence de la plate-forme de l'ennemi (par un système ESM monté sur une plate-forme navale) -- et -- par la surveillance passive de nos bases de défense terrestres -- (le Système ESM peut être monté sur une plate forme aérienne, ou sur un maillage en réseau de systèmes ESM de plate formes terrestres).

Pour reconstituer un environnement électromagnétique , il faut que le signal détecté par les antennes ESM soit parfaitement identifié selon les paramètres ou variables utilisés pour caractériser les signaux, notamment la fréquence porteuse du signal, la direction d'arrivée (DOA), le temps d'arrivée (TOA), la largeur d'impulsion (PW), l'amplitude, le type de modulation d'impulsions (MOP), la forme de l'onde, la modulation en fonction du temps, et en finale connaitre la relation entre l'amplitude et la modulation des ondes continues (CW).

Les équipements ESM ne cessent d'évoluer grâce à une R&D active. Le tout dernier équipement 2015 que les russes possèdent est à un haut niveau de sophistication inégalé, peut ''extraire'' et ''désossé'' tout l'édifice ''connaissance et intelligence'' sur lequel sont bâtis les processus de génération d'ondes des émetteurs ennemis de l'OTAN.

Ces processus de pulsations ou pouls une fois corrélés entre eux, seront regroupés selon un mode complexe par ''famille'' d'ondes, suivant des opérations de tri ou de désentralecement (dans le sens démêler), en anglais interleaving. En raison de la variabilité des signaux, l'extraction automatique est encore rendue très facile par ce nouveau et très récent équipement. Sur des équipements plus anciens, on a constaté que les conclusions faites étaient erronées et fictives, par exemple des émetteurs qui n'existent pas vraiment sont créés par le système ESM ou aussi des fausses alarmes qui sont générées et qui réduisent la fiabilité de l'équipement.

Dans le domaine de l'électronique militaire, l’extraction automatique des signaux ennemis par un équipement ESM est généralement considérée comme un des problèmes le plus ardu et difficile. Dès que les missions SEAD ennemies seront engagées en face de notre DCA et notre aviation, les signaux électromagnétique vont devenir complexe, et doivent être néanmoins extraits à partir d’un monde assimilé à un ‘’fond sidéral électromagnétique’’ (tout juste pour les besoins de l’image), un espace compliqué où les signaux ne sont pas généralement connus à l'avance.

RWR (Radar Warning Receivers, Radars récepteurs d’alerte))

Les principales caractéristiques de l'équipement de cette classe sont la simplicité (Ils mesurent quelques paramètres avec une précision moyenne), une haute fiabilité, un faible poids, et à faible coût.

Ils sont utilisés pour détecter une menace imminente, par exemple, la présence dans une direction donnée d’émission d’un radar sur lequel est pointé un missile qui a verrouillé sa fréquence de travail sur celle d’une plateforme aérienne ou radar de DCA sensé être protégé à terre. Les RWR sont principalement dédiés à la défense de l'avion et permettent au pilote de réagir rapidement soit par une manœuvre d'évitement, ou par deux actions à la fois, une manœuvre d’évitement et le lancement simultané de Chaff (paille), qui se compose de cartouches explosives contenant des millions de minuscules de dipôles, extrêmement légers, capable de générer un très fort écho radar qui masque la plate-forme, ou en générant des signaux de brouillage électronique via un ECM (contre mesure électronique) monté à bord, ou par une combinaison de ces 2 techniques.

ESM-COM

La fonction de ce système est d'intercepter toutes les communications de l'ennemi, localiser l'emplacement des émetteurs et des systèmes de relais radio ensuite détecter et décoder le message lui-même. La connaissance des intentions de l'ennemi est de la première importance pour définir et prendre des mesures opérationnelles appropriées et se positionner aussi sur le choix des contre-mesures électroniques à prendre pour brouiller ou leurrer ses communications.

Infrared Warning (dispositif d’alerte infrarouge).

Les missiles ennemis guidés par rayons infrarouges n’ont pas besoin d'émettre des signaux RF parce qu'ils se verrouillent sur une émission infrarouge naturellement générée à partir de la cible à détruire. Cela signifie que la présence d'un missile infrarouge ne peut pas être détectée, quelque soit la fréquence radio d’un système ESM. En fait, leur détection est normalement obtenue par un radar dédié à l’interception infra rouge appelé OSF (Optronic Secteur Frontal). La volonté de défendre une plate-forme contre les attaques de missiles, cependant, se heurte souvent et rentre en conflit avec la nécessité de maintenir le radar éteint pour éviter la détection par l'ennemi (un '' silence radar ou radio '' de la situation). Dans ce cas, des capteurs électro-optiques passifs offrent une solution alternative. Ce type d'équipement est en fait capable de détecter soit l'échauffement aérodynamique ou le rayonnement infrarouge, produits par le servomoteur du missile au moment de son lancement.

Le problème avec le capteur IF est que son rayonnement infrarouge de fond donne généralement un signal beaucoup plus fort que le signal produit par la menace qui devrait être interceptée. Mais les solutions existent.

Les systèmes qui détectent le rayonnement infrarouge émis au lancement d’un missile sont distincts de ceux qui détectent la chaleur aérodynamique émise en cours du vol. Parmi ces derniers, les systèmes de surveillance de visions infrarouge simple, par exemple, l’image infrarouge frontale (FLIR, Forward Looking Infra-Red) (pour détecter les sources de chaleur et voir la nuit), doivent être distingués des systèmes beaucoup plus complexes et coûteux capable d'avertir automatiquement, appelés veille infrarouge (IRST Infra-Red Search & Track), qui est un système d’imagerie infrarouge, pour la recherche et la poursuite, dont le champ est plus important mais

la fréquence moins élevé.

Les deux systèmes FLIR et IRST sont les deux parties du systèmes OSF (optronic Secteur Frontal). A partir de ces deux voies optroniques, l'OSF assure la détection, la reconnaissance et l'identification à longue portée des objectifs de jour comme de nuit, qu'ils soient aériens, navals et terrestres. Il dispose également les fonctions poursuite angulaire haute résolution et à télémétrie laser.

L'OSF n'émet aucun rayonnement dans son fonctionnement en mode IRST, comme en mode FLIR. De plus, opérant sur des longueurs d'ondes optiques, l'OSF s'avère insensible au brouillage. Totalement intégré au système de navigation et d'attaque de l'avion, il participe à l'information tactique et à l'engagement des cibles en complément du radar, du système de guerre électronique passif et aux liaisons de données.

Laser Warning Receivers (Systèmes lasers récepteurs d'alertes)

La dernière décennie a vu une prolifération d'armes, guidées ou contrôlées par un émetteur laser (ex le missile russe anti char ''Kornet'', guidé par laser a atteint son objectif, avec succès lors des précédentes confrontations opposant la résistance Arabe (2006-2012-2014), contre les Tanks sionistes). Dans la guerre des blindés, des télémètres laser fonctionnent dans un champ de gammes précises, tandis que des lasers cibleurs (calent leur trajectoire sur la fréquence du laser) guident avec précision des bombes ou des missiles vers des cibles au sol. Le laser à dioxyde de carbone permet de guider des missiles à travers des plateformes mobiles et rapides.

Évidemment, la première exigence d'une défense adéquate contre ces menaces est la capacité de détecter leur présence. C'est le rôle des récepteurs d'alerte laser, que les russes ont mis au point pour leur nouveau char… et le char T-90, appelé Shtora-1, un équipement électro-optique actif de protection des blindés, spécialement conçu pour neutraliser le principal missile antichar américain, le BGM-71 TOW. Le Shtora-1 brouille le faisceau laser ou infrarouge du système de guidage des missiles et leur fait manquer leurs cibles. Il brouille également les télémètres laser, les empêchant d'effectuer des mesures correctes de la distance qui les sépare de leurs cibles. Chaque élément de l'équipement comporte quatre paires de capteurs infrarouge et laser couvrant un champ de vision de 360°. La détection de la source de guidage du missile antichar est déterminée avec une précision de 3 degrés. Quatre émetteurs de contre-mesures commencent à créer des impulsions dirigées de brouillage, puis, quand le système de guidage antichar est détecté, intervient le lancement des missiles de riposte. En outre, l'équipement est doté de lance-grenades aérosol qui crée un écran opaque dans le spectre de guidage infrarouge et laser. Les grenades sont lancées à 50-70 m du blindé à protéger. Le Shtora-1 est assisté par un microprocesseur qui reçoit des informations en provenance des capteurs d'alerte et active des contre-mesures.

Notons aussi que les iraniens via Hamas (conflit 2014) sont parvenus a brouillé facilement des systèmes israéliens proche du Shtora-1 en détruisant avec succès une vingtaine de chars sionistes Merkeva de génération 4++ (un dérivé du char américain M1A1 Abrams).

Electronic Countermeasures (contres mesures électroniques).

Après ce bref aperçu des principaux types d'équipements pour la reconnaissance de l'environnement électromagnétique entourant une plateforme ou zone protégée, il est temps de décrire les systèmes dont la tâche est la neutralisation des systèmes électroniques hostiles qui ont été détectés. Leur but est soit de dissimuler la plate-forme protégée ou tromper le système d'arme hostile en créant des cibles parasites.

Chaff (Brouillage mécanique)

Un Chaff est composé d'un nuage de très légères feuilles métalliques en aluminium, des dipôles conducteurs représentés par ces bandes de feuilles de métal utilisées pour créer des zones dans lesquelles le radar est aveuglé et ne peut pas voir les cibles.

Un système de chaff comprend un lanceur qui éjecte des cartouches. Ces cartouches explosent à une certaine distance de la plate-forme protégée et dispersent une multitude de minuscules dipôles dans l'espace. Ces dipôles restent suspendus dans l'espace, produisant un nuage qui sur lequel rayonnent en retour des signaux radar sensés identifier la plateforme (sans toucher la plateforme).

Les Chaffs génèrent de larges couloirs dans lequel les recherches radars sont éblouis et altérées, et ne peuvent pas donc identifier des cibles d'avions, même à des altitudes différentes de celles remplies de chaff. Pour créer ces corridors, les avions volant à haute altitude épandent une énorme quantité de chaff sur une très vaste zone. Parfois, le chaff est lancée à partir d'une plate-forme comme une défense contre un système d'armes offensives. Dans ce cas, le radar du système d'arme est généralement trompé par un fort signal produit par le chaff et est détournée de la poursuite de la vraie cible.

Les corners reflectors (Brouilage mécanique)

Les corners reflectors ont le même effet que les chaffs mais sont de conception très différente. Il s'agit d'objets à faces multiples qui renvoient la plus grande partie de l'émission radar vers sa source. Cependant un avion ne peut pas embarquer autant de corners reflectors que de chaffs.

Decoys (leurres, brouillage mécanique)

Les Decoys sont des leurres, ce sont des objets volants télécommandés destinés à tromper l'opérateur radar en lui faisant croire qu'il s'agit d'un avion réel. Ils sont particulièrement efficaces car ils peuvent saturer un système radar avec de fausses cibles pendant qu'un attaquant s'approche à portée de tir du radar et le détruit. On peut adapter des corners reflectors sur les Decoys pour les faire paraitre plus grands qu'en réalité et les faire mieux confondre avec un avion réel. Pour augmenter leur réalisme, certains leurres ont la possibilité de générer un brouillage radar électronique ou de larguer des paillettes.

Stealth Techniques (techniques de ruse, dissimulation, furtivité)

Naturellement, le meilleur moyen de prévenir la ‘’dangereuse’’ réflexion du signal sur la cible, c’est d’éviter la détection. Étant donné que le signal reçu par un radar est directement proportionnel à la surface équivalente radar (RCS en m²) présentée par la plate-forme cible ; de nouvelle technologie sont développées avec succès pour réduire drastiquement la force du signal de radar produit par la plate-forme protégée.

A cette fin une nouvelle technologie a été développée au cours des 20 dernières années pour l'étude des matériaux et des géométries structurelles capables de minimiser la surface équivalente radar de la cible. Les techniques qui leur sont inhérente sont généralement appelées des techniques de furtivité, de ruse ou dissimulation (Stealth). Ils sont très prometteurs; les partisans de l'avion furtif aux États-Unis l’appellent '' l’avion invisible '' (la ‘’furtivité’’ n’existe pas si on est en possession d’une variété de radars disposés de façon optimale sur le territoire et si possible reliés à une détection aérospatiale (radio fréquence et optronique), les chinois et les russes arrivent à profusion à détecter les F 22 et F 35 américains sensés être furtifs).

Noise Jammers (Brouillage par bruit électronique).

Le but d'un brouilleur d’ondes est de masquer les cibles par des émissions de signaux qui ont pour fonction d’entretenir de la confusion sur l'écran radar intercepteur.

Un brouilleur génère des signaux à la même fréquence que le radar adverse. Ces signaux créent une perturbation équivalente à un très fort bruit thermique dans le récepteur radar. Ainsi, le signal produit par la plate-forme est noyé dans le bruit et ne devient plus '' visible ''

Deception Jammers (Brouillage électronique par fausses cibles)

Une des fonctionnalités additive d'un brouilleur est de générer des signaux pour ruser et tromper, dans le but de protéger une plate-forme en attirant les radars ennemis vers de fausses cibles (imaginer la situation ou quelqu'un est situé à gauche de votre oreille mais vous l'entendez par l'oreille droite, ou vous croyez l'apercevoir en face de vous mais réellement est derrière vous, ces feintes ou ruses sont fréquemment utilisées en guerre électronique, mais les parades existent pour les déjouer).

Un brouilleur de Deception (de l'anglais, ruser , tromper) génère aussi de cibles virtuelles radar, ce qui va empêcher un radar de recherche d'identifier la véritable plate-forme. Dans ce cas, le relais et le suivi sera assuré par les radars de poursuite, malgré que le système d'armes (lié au radar intercepteur) est verrouillé et qui se déplace progressivement vers la fausse cible.

De nos jours, de nombreuses techniques existent pour tromper (et non plus "brouiller") un radar. En gros, on peut citer :

- lui donner de fausses infos sur la position, l'altitude, la vitesse et le cap de la cible. Pour ce faire, on manipule l'écho ou on en fabrique un nouveau, ou les deux à la fois. "Range gate pull-off" fait partie de ces techniques.

- De la même manière, on peut manipuler un écho en y incluant électroniquement certaines données mathématiques qui feront "loucher" le radar lorsque celui-ci tentera d'interpréter les données. Le terme anglo-saxon est Cross-Eye jamming .

- Gaver le radar avec tant de vraies données répétées à l'infini que celui-ci "Pète un plomb" (hack-attack ou "soft-kill")

- Effacer purement et simplement l'écho radar.

ECM-COM

Le but de ces systèmes est de générer des signaux de bruit ou des interférences, afin de bloquer les récepteurs de systèmes de télécommunications de l'ennemi, rendant ainsi les messages incompréhensibles. L'incapacité à lever ces perturbations voir l'arrêt sur les systèmes de communication d'une armée est un inconvénient majeur sur les champs de bataille (mais les parades pour y faire face, existent).

Infrared Countermeasures (IRCM)- contre mesure infrarouge

Ce sont des systèmes qui empêchent les missiles guidés par infrarouge d'atteindre la cible (Manpads, tel les Igla russes). Actuellement, il existe deux types de systèmes: à bord et hors-bord de la plateforme visée.

Le système de défense à bord est composé d'émetteurs infrarouges modulés. L'équipement qui recherche les rayons infrarouges est très souvent basé sur un système de suivi à balayage, qui émet un signal infrarouge modulé en amplitude visant à introduire des erreurs énormes dans une trajectoire de missile. Le système off-board est un distributeur d'un essaim de fusées thermiques (flare dispenseur), ce sont des cartouches (comme un feu d'artifice) éjectées de la plateforme aérienne qui génèrent un rayonnement infrarouge intense pour tromper le détecteur de chaleur de missiles hostiles.

ECM-Lasers (contre mesure electronique laser)

Des systèmes de lasers sont déployés sur la plateforme pour faire barrage à toute une panoplie de faisceaux lasers qui menacent la plateforme. Ils utilisent les mêmes principes de fonctionnement que les brouilleurs

mentionnés ci-dessus en propageant des nuages de fumée qui réduisent la visibilité afin altérer le ciblage laser.

Electronic Counter-Countermeasures (ECCM, contre-contre mesure électronique).

Ces dispositifs sont généralement ajoutés aux capteurs des missiles ou d'autres armes pour leur permettre de fonctionner dans un environnement électromagnétique hostile auto-entretenu par des brouilleurs adverses, visant à réduire drastiquement l'efficacité usuelle de ces derniers.

Dr Mohamed Belhoucine

(*): Les contributions publiées sur Liberte-algerie.com relèvent exclusivement de la responsabilité de leur auteurs