La guerre électronique [suite]

Autor(en): **Trichet, J.C.**

Objekttyp: **Article**

Zeitschrift: **Pionier : Zeitschrift für die Übermittlungstruppen**

Band (Jahr): **60 (1987)**

Heft 11-12

PDF erstellt am: **09.08.2024**

Persistenter Link: https://doi.org/10.5169/seals-561541

La guerre électronique (II)

Bavarder discrètement et voir mine de rien

par J. C. Trichet

Depuis qu'ils en maîtrisent l'usage, les militaires ne voient pas comment se passer du spectre hertzien. Au contraire, ils recherchent de nouvelles plages de fréquences, abordant la frontière du spectre visible. Déceler les émissions adverses, analyser ce qu'elles véhiculent comme informations, les noyer sous un bruit artificiel, détruire les émetteurs, voir s'immiscer dans les communications adverses: telles sont les tâches des contremesures électroniques. Pour y parer, on recourt à un ensemble de techniques: ECCM.

Définir les menaces

Toute riposte ne pouvant être efficace qu'à mesure d'une connaissance parfaite de la menace, il importe de bien savoir comment travaillent les ECM dont on veut s'affranchir. Les plus difficiles à déjouer sont les moyens d'écoute et d'analyse, qu'on réunit sous le nom générique d'Elint (intelligence électronique). En pratique, on se comporte en partant du principe qu'on sera forcément détecté et suivi à un moment ou un autre, et on en tient compte dans le processus d'émission.

Le brouillage, c'est-à-dire les ECM actives, est plus facile à déceler, donc à contrer. On peut s'en prémunir soit en détruisant le brouilleur, soit en le leurrant, soit encore en modifiant la forme de l'émission de façon à surprendre le brouilleur, soit enfin en adaptant la réception pour en extraire le signal utile dans le fouillis créé par le brouilleur.

Discrétion: tel est le leitmotiv de l'électronicien qui recherche le moyen d'éviter au maximum la détection d'une émission. Cette discrétion s'obtient essentiellement en émettant une puissance minimale pendant le temps le plus court possible. Elle peut également passer par une évolution continuelle et déroutante – pour l'écouteur – de la fréquence d'émission. Enfin on peut aussi délocaliser l'émission en la répartissant entre plusieurs émetteurs travaillant en réseau maillé.

Outre le fait qu'elle réduit les risques d'être brouillé, la discrétion d'un émetteur lui apporte une bonne marge de survie contre les possibilités de destruction par missile antiradiations. Cependant, la discrétion absolue reste impossible, dès lors que l'ennemi dispose de suffisamment de temps pour détecter une émission. Il faut donc s'arranger pour que la détection d'une émission apporte à l'indiscret un minimum d'informations sur l'origine de cette émission, et si possible que le contenu de cette émission reste secret, dès lors qu'elle porte des informations dont l'exploitation nuirait aux forces ainsi espionnées à leur insu.

Là réside le principal «challenge» à relever par les concepteurs d'ECCM: compliquer et rendre la plus imprécise possible la localisation géographique d'une source d'émission, d'une part, permettre en tout état de cause le portage des informations par la source d'émission, au profit de ceux auxquels elle est destinée et à eux seuls, d'autre part.

On comprend alors que le travail ECCM commence dès le stade du renseignement stratégique, – à travers l'Elint et plus généralement de qu'on appelle «guerre électronique». Connaître les matériels d'émission que l'adversaire potentiel peut mettre en œuvre, savoir où ils se trouvent et quel espace ils couvrent – géographique et dans le spectre hertzien: telle est la tâche, dès le temps de paix, des moyens d'espionnage électronique (avions, navire, véhicules divers et satellites). Pour déjouer cette écoute permanente, on garde en réserve des moyens d'émission qui ne se dévoileraient qu'au tout dernier moment, pratiquement à l'instant de la frappe. C'est ainsi, par exemple, que les radars modernes comportent des modes de modulation «secrets», qu'on n'active même pas lors des exercices en temps de paix et qui ne sont mis en œuvre – à l'insu souvent de l'opérateur lui-même – que sur un ordre crypté.

Pour obliger l'ennemi potentiel à dévoiler ces procédures d'émission les plus secrètes, certains n'hésitent pas à risquer le sacrifice d'avions-espions avant de prononcer une attaque; quant on ne voit pas, en temps de paix, des opérations de provocation à l'extrême limite du casus belli.

Préserver l'essentiel

En matière de transmissions comme pour le radar, il n'existe aucune parade ECCM totale et parfaite. Ceci posé, on s'efforce donc, soit de garantir une protection absolue dans des conditions bien définies – sur un laps de temps ou à l'intérieur d'un espace circonscrit –, soit de conserver un minimum de fonctions en ambiance de contre-mesures, afin de maintenir le déroulement de la mission principale, tout en admettant d'abandonner alors la ou les missions secondaires. Dans cette optique d'ailleurs, une tactique ECCM couramment employée consiste à faire prendre à l'ennemi une mission secondaire pour la mission principale, afin qu'il affecte tout son potentiel ECM à la première, laissant la seconde libre de s'exercer.

Compte tenu de la diversité des missions réalisables par les systèmes d'armes modernes, comme un avion d'attaque, il importe de donner à ces systèmes une capacité à se reconfigurer pour conserver un potentiel suffisant en cas de contre-mesures. Les systèmes numériques offrent une grande aptitude en ce sens puisque leur mode opératoire peut être configuré par logiciel. A condition cependant qu'on ait conçu le matériel pour qu'il conserve une efficacité optimale avec des logiciels évolutifs. Dans tous les cas, on aboutit à un compromis, ce qui rend très difficile l'adjonction de fonctions ECCM en «rétrofit» sur un système existant.

C'est ainsi qu'on s'efforce d'assurer une protection maximale à la fonction «poursuite» d'un radar d'intercepteur, en admettant que les fonctions «recherche» soient dégradées par brouillage. Cette protection peut d'ailleurs découler d'une procédure rendant difficile, voire impossible, la discrimination entre poursuite et recherche; ce qui est l'un des objectifs des radars à poursuite sur informations discontinues (track-while-scan). Outre la protection réalisée par l'équipement détecteur lui-même, on peut concevoir une protection au niveau de système global: passage en poursuite sur navigation autonome pour un missile dont l'autodirecteur est brouillé; appui d'une détection optronique pour suppléer les sens défaillants d'un radar brouillé. Pour en équipement de transmission, la protection ECCM consiste avant tout à garantir que le message porté sera bien correctement reçu par son destinataire; et si ce message est confidentiel – ce qui n'est pas toujours le cas – il importe qu'on ne puisse l'intercepter et le comprendre. A contrario, il ne faut pas que l'ennemi puisse s'immiscer dans la liaison pour y faire transiter des messages-leurres qui seraient crédibles. Ces notions sont importantes, car elles expliquent l'importance des progrès obtenus grâce à des techniques modernes, telles que l'étalement de spectre ou l'évasion de fréquence, qui permettent de préserver l'intelligibilité d'un message pour son destinataire, et pour lui seul, à travers un puissant brouillage. Au passage, notons que ces techniques imposent à l'ennemi de recourir à des procédés de brouillage de plus en plus puissants, donc plus facilement localisables et plus exposés à la destruction.

Des yeux plus malins

La protection des systèmes de détection et de conduite de tir commence au stade de leur conception globale. C'est ainsi que face aux progrès des ECM, et spécialement des leurres, on développe une génération de systèmes combinant radar et optronique; caméras TV ou thermiques, senseurs infra-rouges viennent alors épauler le travail du radar, obligeant l'ennemi à déployer une panoplie de moyens de contre-mesures couvrant les plages de fréquences et les modes opératoires de tous ces systèmes.

On imagine que l'emport de cette panoplie n'est guère possible à bord de porteurs offensifs de taille limitée et, en tout état de cause, que ces moyens diversifiés de contre-mesures rognent sur la capacité d'emport d'armements et/ou le rayon d'action des porteurs; sans parler de leur extraordinaire renchérissement, qui les rend alors justiciables de l'emploi d'armes plus coûteuses, donc encore plus difficiles à leurrer ou brouiller. On touche là, d'ailleurs, un point sensible de la lutte ECM/ECCM: le prix à payer, qui constitue aujourd'hui la limite opérationnelle, quand la technique permet en fait pratiquement les combinaisons les plus complexes.

L'association d'un radar et d'un détecteur optronique permet en outre de surveiller, et éventuellement de riposter, contre une contre-mesure. Ainsi, le radar brouillé peut passer sur

un mode de veille assurant la poursuite du brouilleur tandis que l'optronique prend le relais pour maintenir le contact avec le but. La technologie des antennes à balayage électronique apporte une autre solution, puisqu'elle permet de générer plusieurs pinceaux, aptes à évoluer chacun pour leur compte, dans l'espace comme dans le spectre de fréquences. Ainsi, tandis qu'un ou plusieurs faisceaux sont brouillés, d'autres maintiennent leur poursuite des objectifs et d'autres encore déterminent la position du brouilleur dont on peut alors régler le compte!

Toutefois, le passage d'un mode de travail normal à un mode plus complexe en réaction à une contre-mesure ne s'effectue pas aussi simplement qu'il y paraît. Dans tous les cas – sauf à surdimensionner le système dans des proportions impensables – il faut accepter une dégradation de ses performances globales. Par exemple, l'efficacité d'une combinaison radar + optronique n'est optimale que lorsque le système de contre-mesures se déclenche à une distance située à mi-chemin entre la portée maxi du radar et celle de l'optronique.

En fait, la mise en œuvre des moyens de ECCM nécessite souvent l'appréciation d'un opérateur spécialisé et entraîné. Or c'est impossible dans certaines conditions, par exemple à bord d'un avion monoplace. D'où l'étude de systèmes aptes à adapter eux-mêmes leur fonctionnement en environnement ECM. Il s'agit d'abord de laisser croire au brouilleur qu'on n'a pas découvert son activité, en continuant à faire «comme si», mais en prenant discrètement les mesures nécessaires pour continuer à garder la cible à l'œil.

Forcément, on débouche ici sur les applications de l'intelligence artificielle, où un système expert contrôlera les modes opératoires du radar (sauts de fréquences, changements des largeurs d'impulsion et fréquences de récurrence), tandis qu'un autre système expert peut programmer les modes de balayage de l'antenne. Bien entendu, tout en adaptant ainsi le système à l'environnement hostile qui lui est imposé, le système expert doit informer le pilote de la situation. D'une part il lui indiquera la présence de la contre-mesure; d'autre part il l'informera de la mise hors disponibilité des fonctions oblitérées par les ECM, ainsi que de la réduction des performances de son système de conduite de mission, découlant des choix effectués automatiquement pour faire prévaloir la priorité opérationnelle du moment.

On en arrive actuellement à envisager un système d'antenne à balayage électronique piloté par I. A., capable de donner à une cible l'impression qu'on ne l'a pas vue, alors qu'on la traque discrètement. Ceci peut s'obtenir en théorie si le temps d'éclairement de la cible reste, à chaque passage, inférieur au temps de réaction du détecteur ECM; ce qui, en pratique, impose un changement de fréquence et/ou du mode impulsionnel à chaque balayage de la même cible, selon une loi aléatoire aux yeux du détecteur. Un tel processus de travail donne d'ailleurs au radar une très grande protection contre les missiles antiradiation, incapables – dans l'état actuel de la technique – d'emporter des auto-directeurs doués d'une faculté d'adaptation aussi étendue et rapide que le radar qu'ils espèrent détruire.

Les vocalises du bègue bavard

Les possibilités de l'intelligence artificielle vont également être mises à profit pour donner une fonction ECCM performante aux systèmes de transmissions. On leur confiera en effet la gestion des processus ECCM déjà connus, spécialement de l'évasion de fréquence et de l'étalement de spectre. Notons que les équipements les plus modernes comportent déjà, au niveau du traitement à la réception, un certain degré d'intelligence qui permet d'adapter la loi de décryptage d'un message noyé dans du bruit aux caractéristiques de celui-ci, qu'il s'agisse de bruit naturel ou provoqué.

En matière de télécommunications, la protection ECCM pose un dilemne: obtenir un rapport signal utile/bruit maximal tout en réduisant au minimum l'apitute à détecter le signal utile; ou encore réduire la bande passante du détecteur tout en élargissant au maximum la bande d'émission, afin de saturer l'espace hertzien proposé aux brouilleurs éventuels. On n'a pu contourner ces contradictions qu'avec l'avènement des systèmes numériques qui permettent de distribuer un message par paquets minuscules à travers une large bande du spectre.

C'est d'abord l'objet du saut de fréquence programmé par un code. Compte tenu de l'émergence d'une génération de brouilleurs «suiveurs» ultra-rapides, la complexité du code pseudo-aléatoire gouvernant le programme des sauts de fréquence passe maintenant après la vitesse des sauts. En pratique, on admet qu'un système changeant de fréquences dix fois plus vite qu'un détecteur est bien protégé contre les ECM. Sous réserve encore que le système balaie un spectre très large, qui obligerait l'ennemi, soit à mobiliser une armée de brouilleurs calés sur un très grand nombre de fréquences, soit à employer des brouilleurs à très large bande, coûteux et nécessitant une énorme puissance d'émission. L'étalement de spectre consiste à appliquer au signal utile par une modulation biphase générée selon un code pseudo-aléatoire. L'utilisation de la même séquence pseudo-aléatoire à la réception permet de retrouver le signal portant le message utile. On combine ainsi une émission dans une large bande avec un signal utile maintenu dans une bande très étroite.

Enfin, on peut effectuer, à la réception, un traitement statistique du signal, selon une technique de filtrage adaptatif. Ceci nécessite un dispositif apte à «apprendre» le bruit qui noie le signal à détecteur. En pratique, cet apprentissage s'effectue sur un message de référence qui est généralement le message de synchronisation nécessaire pour la transmission en saut de fréquence.

Cette technique apporte des résultats très spectaculaires pour la protection contre les brouilleurs à bruit blanc, qui constituent les «suiveurs» les plus rapides (puisque les brouilleurs «copieurs» doivent d'abord «apprendre» le signal à brouiller). Elle s'avère également fort efficace lorsque le brouillage se situe en limite de portée, ce qui accroît la portée opérationnelle d'un système ou permet de la faire travailler en puissance réduite dès qu'on se rend compte qu'il est brouillé.

La combinaison des trois techniques permet d'obtenir des gains signal utile/puissance de brouillage très élevés. En théorie, dans la technologie actuelle, un gain de l'ordre de 80 dB est parfaitement réalisable. Même en tenant compte de l'effet de la directivité des antennes des brouilleurs, on obtient encore une protection fort élevée, puisque certains systèmes s'avèrent capables de résister, avec un émetteur de 1 W, à un brouilleur de quelques 40 MW!

Les évolutions de technologie des circuits intégrés à très grande vitesse vont plutôt dans un sens favorable aux techniques ECCM. On sait par exemple réaliser des modulateurs donnant des sauts de fréquence à une cadence de 2000 à 3000/s; dépassant très largement les capacités de poursuite des brouilleurs bruit blanc connus et tout à fait hors de portée actuellement des techniques de brouilleurs-suiveurs.

Quant aux générateurs de codes pseudoaléatoires pour l'étalement de spectre, disons qu'un simple générateur séquenciel à 31 portes suffit pour obtenir une séquence de 2 millions de bits; en attaquant ce générateur avec une horloge de commande à 1 MHz, la séquence ne se reproduira que toutes les 33 secondes; délai qui peut être porté à des semaines, voire à des années simplement en connectant plusieurs générateurs en cascade.

Toutefois, la limite technologique de ces systèmes se trouve dans les possibilités de synchronisation du/ou des récepteurs, qui doivent d'abord se caler sur le code de l'émetteur afin de retrouver le message utile. Outre l'emploi d'horloges ultra-précises, associées à des synthétiseurs ultra-rapides, (on travaille ici sur les circuits intégrés hybrides à processeur optiques), on peut tourner le problème en employant une clé de code discrète qui, par déduction mathématique, permet de retrouver rapidement la séquence de modulation pseudo-aléatoire.

On sait aujourd'hui employer des codes portés par des processeurs 64 bits, donnant une protection efficace pendant une semaine, au cours de laquelle seuls les récepteurs porteurs de ce processeur pourront comprendre ce qu'on leur dit; même si l'ennemi, ayant réussi à enregistrer l'intégralité d'un message, le «travaille» sur le plus puissant des ordinateurs actuellement connu.

En somme, au lieu de l'antique «silence radio», on encourage au contraire les systèmes modernes de transmission à saturer au maximum la bande hertzienne, en s'y promenant le plus vite possible, un peu à la manière d'un ténor bègue qui s'efforcerait à vocaliser sur 8 octaves!

De tels progrès permettent aujourd'hui aux forces engagées en opération de rester en contact radio sans risquer de voir l'ennemi intercepter les messages échangés, si même il s'avère capable de les brouiller. En combinant cette capacité ECCM à des moyens d'oblitération des émetteurs de contre-mesures, on a vu récemment certaines armées (notamment Tsahal) se permettre d'accaparer à leur profit le spectre hertzien au moment le plus crucial d'un engagement.

Dans le domaine du radar, les procédures ECCM portées par logiciel expliquent l'importance et le niveau de confidentialité attachés aux travaux des logiciens militaires. Plus encore, ceci démontre qu'on conserve un «droit de regard» sur l'emploi de matériels livrés à des pays tiers, au cas où ces pays se risqueraient à mettre ce matériel en œuvre contre les forces de celui qui le leur a livré ou d'un de ses alliés.

Ainsi exprimés, des implications profondes des techniques ECCM placent ce domaine dans la frange la plus confidentielle des travaux militaires, du fait de leurs effets politiques et stratégiques.

(Article gracieusement mis à disposition par Stephane Ferrard, rédacteur en chef de DEFENSE & ARMEMENT incorporant la revue Heraclès, et paru dans le numéro de Mars 87 N° 60) Copyright Defense et Armement, Paris.