



Le mot  
du Président

*Chers amis,*

*Il y a un peu plus de deux ans, l'Association Guerrelec élargissait son périmètre et s'ouvrait au Cyber. Le concept de supériorité des forces par la maîtrise de l'information développé par le SACT (Supreme Allied Command Transformation) de l'OTAN a démontré toute sa pertinence. La circulation de l'information qui est au cœur de tous les systèmes, qu'ils soient tactiques ou stratégiques, est menacée aujourd'hui à tous les niveaux, que ce soit dans son transport via les ondes hertziennes par les moyens de Guerre Electronique conventionnels ou au niveau de la manipulation de l'information elle-même (usurpation d'identité, déni d'accès, hacking, phishing, ...). C'est donc au service de cette problématique globale que Guerrelec se propose d'apporter son soutien, en promouvant tous ceux qui, en France étatiques et industriels, œuvrent à sa résolution.*

*Dans cette nouvelle lettre vous découvrirez des articles sur l'élargissement de la GE, puis l'aérocombat en action entre 2011 et 2013, la dernière campagne EMBOW 14 à Biscarosse, l'escapade de Guerrelec tout près des plages du Débarquement pour marquer le 70<sup>ème</sup> anniversaire du Débarquement, les derniers potins de l'été en matière de GE et enfin le 51<sup>ème</sup> AOC à Washington.*

*Et n'oubliez pas notre séminaire du 26 novembre prochain sur le thème **Comment rester maître de l'Ether et du Cyberspace ?***

*Bonne lecture à tous,*

IGA Pierre **GRANDCLEMENT**  
Président de Guerrelec

## L'élargissement de la notion de Guerre Electronique à la Guerre Informatique ou Cyber défense

La GE, c'est priver l'adversaire de l'usage du spectre électromagnétique au sens large... De plus en plus, il devient nécessaire d'expliquer l'élargissement de la notion de Guerre Electronique à la Guerre Informatique ou Cyber défense. Cette évolution logique doit restée centrée sur les systèmes d'armes et systèmes d'information opérationnels.

La Guerre Electronique opère jusqu'à présent dans le milieu des ondes et de leur transmission. Les modes opératoires vont de l'écoute jusqu'au brouillage et au leurrage, et ce, dans les domaines EM<sup>1</sup>, IR<sup>2</sup>, Laser et/ou UV<sup>3</sup>. Le but final est alors la recherche d'information sur l'ennemi, sa localisation et la perturbation du guidage de ses armements. Mais, avec l'évolution technologique, théorisée notamment par la révolution dans les affaires militaires (RMA), les systèmes d'armes modernes sont devenus fortement dépendants des systèmes d'information qui, soit les constituent intrinsèquement, soit les relie aux diffé-

rents centres C2<sup>4</sup>. La recherche d'efficience implique donc de se pencher sur l'attaque de cet aspect informatique des systèmes d'armes, afin de faire le point sur l'intérêt de ce côté « soft<sup>5</sup> » de la Guerre Electronique...

### Optimiser pour mieux lutter

Dans la bataille sans fin du glaive contre la cuirasse en matière de Guerre Electronique, les progrès des systèmes d'armes nécessitent une évolution constante et coûteuse des équipements de détection, de brouillage et d'autoprotection (des navires, aéronefs,...). Cependant les technologies récentes des radars et autodirecteurs riment avec réseaux, maillage, transmission de l'information qui permettent d'augmenter les portées, d'optimiser les détections, de diminuer le temps de décision et de réaction. Les systèmes d'armes modernes, en particulier anti-aériens, s'inscrivent donc dans un schéma technique qui vise à accélérer et optimiser

sans cesse la boucle OODA (Observation, Orientation, Décision, Action). Ainsi parallèlement à l'attaque directe par brouillage d'un radar ou d'un autodirecteur toujours plus complexe, l'autre aspect de la lutte contre un système d'arme revient à traiter son système d'information et de communication. Le but est alors soit de le rendre inopérant, soit de l'isoler en « cassant » la boucle OODA, par une attaque électronique et informatique adaptée.

## L'évolution technologique et informatique crée potentiellement de nouvelles failles

En effet, si la technologie numérique apporte un gain considérable en termes d'efficacité pour l'exécution des missions et la précision des armements, elle peut aussi générer des failles qui n'existaient pas auparavant. Ainsi la généralisation des systèmes d'information au sein des systèmes de combat crée dans l'absolu l'opportunité d'attaques informatiques auxquelles les générations précédentes de matériels ne pouvaient être sensibles.

On peut lire de cette façon dans *Air Forces Monthly*<sup>6</sup> : « On avait l'habitude de dire que l'Avro Shackleton (NDLR : avion de patrouille maritime britannique entre 1950 et 1990) était un vol en formation serrée d'un million de rivets - aujourd'hui un F-35 Lightning II peut être assimilé à 1 500 ordinateurs embarqués et 600 éléments de cryptage (lien de communications sécurisées) volant en formation serrée ». Soient autant d'éléments susceptibles d'être attaqués numériquement. Il en est de même pour les liaisons de données qui lient aujourd'hui les systèmes d'armes en eux.

Le 6 septembre 2007, des appareils israéliens ont ainsi fait une incursion particulièrement discrète en territoire syrien afin de détruire un réacteur nucléaire d'origine nord-coréenne. Le système C2 de défense aérienne s'est révélé alors étonnamment inopérant. Si les pays impliqués se sont montrés plutôt muets sur cette opération, de nombreux articles ont avancé l'idée qu'aux côtés d'actions de brouillage et de SEAD<sup>7</sup> classiques une attaque électronique et informatique des liaisons entre les C2, très centralisés, aurait permis un tel résultat...

De la même manière, l'utilisation d'un drone, de plus en plus prégnante dans les conflits actuels, reste tributaire de la liaison de données qui le lie à son pilote au sol. Ce système est aussi dépendant de la qualité de sa géo-localisation et, donc, de la qualité du signal GPS reçu. Ces éléments représentent autant de vulnérabilités que les Iraniens semblent avoir exploitées lors de la capture d'un RQ-170 *Sentinel* en décembre 2011. De nouvelles possibilités d'attaque et de neutralisation des systèmes d'armes, liées aux systèmes d'information, apparaissent donc dans le combat moderne.

## Limiter les fantasmes dans le domaine

Il faut cependant se garder des fantasmes véhiculés par les cinéastes et les médias concernant les attaques informatiques sur des systèmes d'armes opérationnels. Il est important de différencier l'informatique bureautique classique plus ou moins reliée à internet, des systèmes d'informations spécifiques couplés à un système d'armes. Dans le premier cas, les vulnérabilités sont celles auxquelles tout un chacun est confronté au quotidien, à savoir les virus et autres *chevaux de Troie* s'infiltrant dans un PC. Et cela représente une lutte et une vigilance de chaque instant à

tous les niveaux, comme en témoigne l'affaire en mars 2011 du vol de données à grande échelle, via une infection virale, sur des ordinateurs de Bercy.

Dans l'autre cas, on imagine mal un « hacker<sup>8</sup> », via son poste internet ou une clé USB, infecter simplement le SNA<sup>9</sup> d'un avion de combat pour le rendre inopérant, même si cette image, dont le contour reste assez flou pour la plupart en l'absence des connaissances techniques idoines, est largement relayée dans les films américains. C'est ainsi qu'un groupe de hackers dans « Die Hard 4 » détourne de sa mission un F-35 en infiltrant sa liaison de données ou que Will Smith dans *Independence Day* va inoculer, via un Mac portable, un virus dans une soucoupe volante.

## La réalité des choses aujourd'hui

Le « hacking » d'un système d'information opérationnel, spécifique, lié à un système d'armes physique et, donc, destiné à opérer des machines sophistiquées en temps réel, ne présente pas la même complexité que la création par un hacker d'un virus générique destiné à contaminer un PC standard. Les programmes malveillants conçus pour ordinateur fonctionnant sous Windows étant déjà inopérants sur un Mac (et vice versa), il est aisé d'imaginer la difficulté de mettre en défaut des machines robustes et dédiées à un usage particulier.

Il existe cependant un exemple connu : la fameuse attaque du ver « Stuxnet » qui, à l'automne 2010, s'en est pris aux machines Siemens qui contrôlaient les centrifugeuses du programme nucléaire iranien. Ce code malicieux s'est répandu sur ces équipements (via les ordinateurs sous Windows qui géraient les automates programmables industriels de Siemens), pour amener des effets physiques par dérèglement des centrifugeuses ainsi pilotées, avec à la clé de réels dégâts matériels, de l'aveu même des Iraniens. Si cette attaque informatique a bien obtenu les effets escomptés, le virus généré a nécessité, d'après la firme de sécurité Symantec, le travail d'une équipe de 5 à 10 personnes pendant 6 mois. La complexité du code suggère le travail d'une équipe professionnelle, probablement étatique, et qui connaissait parfaitement le système Siemens visé.

Car c'est ici que réside la principale différence entre une attaque informatique classique et celle visant un système opérationnel contrôlant des machines physiques : il faut maîtriser complètement le système très spécifique visé, dans son fonctionnement, son codage, et surtout le moyen d'y entrer, pour pouvoir prétendre à une éventuelle efficacité. Cependant l'exemple précédent montre aussi que l'utilisation, souvent pour des raisons de coût, de temps, de simplicité et d'interopérabilité, de systèmes d'exploitation classiques comme support aux applications opérationnelles, en augmente aussi la vulnérabilité. **Ces considérations limitent donc le champ d'action d'une attaque informatique visant un système d'armes, la restreignant à un moyen d'appoint contre des systèmes bien connus de l'assaillant et pourvus de failles exploitables de l'extérieur.**



Ce n'est pas encore demain la veille que ce genre « d'attaque » se produira... (Photo Fabrice Cinquetti).

1 EM : électromagnétique,  
2 IR : infrarouge  
3 UV : ultraviolet  
4 C2 : command and control  
5 Soft : logiciel  
6 Cyberspace, the new battleground, Air Forces Monthly avril 2012, par Andrew Brooks

7 Suppression of Enemy Air Defense  
8 Hacker : pirate informatique  
9 SNA : système de navigation et d'attaque  
10 Aviation Week, 16 janvier 2012, Electronic Warfare, Israeli Angst, by Alon Ben-David  
11 Il devient difficile de séparer la Guerre Informatique de la Guerre Électronique tant les deux domaines interagissent.

## L'avenir dans la Guerre électronique et numérique

Il s'avère donc que l'attaque informatique et électronique des systèmes d'information associés au système d'armes constitue une voie de recherche intéressante, mais, loin des idées confuses et populairement admises, nécessite des connaissances et des renseignements au moins aussi poussés que pour la Guerre Electronique plus classique. Cependant les efforts se multiplient dans le domaine. Après le Cyber Command américain, les Britanniques se sont dotés du UK Defence Cyber Operations Group et la France réalise notamment la montée en puissance du pôle de cyber défense de DGA/Maîtrise de l'information. Est-ce un hasard s'il est ainsi co-localisé avec le centre d'expertise en Guerre Electronique de la DGA ? *Aviation Week*<sup>10</sup> cite ainsi une source industrielle israélienne: « **It's becoming hard to separate cyberwarfare from electronic warfare as the two realms closely interact** »<sup>11</sup>.

## L'aérocombat en action

Le 7 juillet 2014, nous avons reçu dans le cadre de notre cycle de conférences, colonel Frédéric Turquet, chef du « bureau études prospective » (BEP) du COMALAT. Il a notamment commandé le 3<sup>ème</sup> RHC à ETAIN entre 2011 et 2013, période durant laquelle son régiment a été engagé en Afghanistan et en Libye, avant de rejoindre COMALAT.

La conférence présentée a porté sur « l'aérocombat en action » et a été illustrée par quatre opérations récentes et emblématiques des engagements de l'ALAT :

- |                    |                       |
|--------------------|-----------------------|
| RCI (2011)         | • Opération LICORNE   |
| Afghanistan (2011) | • Opération PAMIR     |
| Libye (2011)       | • Opération HARMATTAN |
| Mali (2013)        | • Opération SERVAL    |

L'ALAT célèbre cette année ses 60 ans, à comparer aux 30 ans de l'Army Aviation US et aux 80 ans de l'armée de l'air française. L'ALAT est la première flotte d'hélicoptères d'état en France : ses 330 hélicoptères de combat représentent 55 % de la flotte d'état. L'expertise « hélicoptère » se trouve au sein de l'armée de terre. L'ALAT française est aujourd'hui reconnue dans le monde comme la deuxième ALAT (derrière l'Army Aviation US) et la première en Europe (devant l'armée britannique).

Dans sa dimension « force de combat », l'ALAT ce sont 3800 hommes et 200 hélicoptères de combat répartis au sein de 4 régiments dont un dévolu aux Forces Spéciales et structurés en bataillons : 1 bataillon d'hélicoptères de reconnaissance et d'attaque (BHRA), 1 bataillon d'hélicoptères de manœuvre et d'assaut (BHMA) et 1 bataillon d'appui aéromobile (BAA).

Le domaine d'évolution des hélicoptères de l'ALAT se situe dans une frange située principalement entre 0 et 50 m/sol : les hélicoptères sont totalement intégrés à la manœuvre terrestre et constituent un des trois pions de manœuvre du chef tactique interarmes. On parle « d'aérocombat ».

L'aérocombat est un concept qui consiste en l'intégration des tactiques, des missions et des modes d'action aéromobiles à la manœuvre terrestre en étroite coordination et combinaison avec les deux autres composantes de la fonction contact que sont le combat embarqué (cavalerie blindée) et le combat débarqué (l'infanterie). Les unités aéromobiles sont indissociables de la manœuvre aéroterrestre et s'intègrent dans la structure quaternaire interarmes. Dans ce cadre, les unités aéromobiles peuvent intervenir de multiples façons, en offensif ou défensif, en premier échelon ou en deuxième échelon.

Le commandement des unités aéromobiles est assuré par des HMA PC GAM qui peuvent se situer jusqu'à 100 km de sa base arrière et commander des SGAM situés à 30 km en avant.

Le ciel et l'espace ne véhiculent donc plus seulement des watts, mais aussi des données ! S'il est indéniable que la guerre de transmission de puissance électromagnétique, IR ou laser, garde et développe plus que jamais toute sa pertinence, il ne faut pas négliger l'essor de ce nouvel aspect que représente l'attaque du contenu numérique des ondes émises et des systèmes d'information associés aux systèmes d'armes.

Ainsi la Guerre Electronique se pare d'une autre facette qui densifie encore un peu plus la complexité du combat de demain.

Lieutenant-colonel Fabrice **Cinquetti**,  
en charge des affaires de GE au bureau expertise organique,  
programmes de l'EMAA



En opérations au Mali (Photo colonel Turquet)

Ceci permet d'avoir une élongation d'environ 150 km entre la grande unité et les hélicoptères engagés les plus éloignés. Sur cette distance, les unités aéromobiles sont en mesure d'assurer leur soutien logistique par la mise en œuvre de plots de ravitaillement (FARP) alimentés par des bacs souples transportés par HMA. La patrouille d'hélicoptère est le maillon indissociable dont la composition mixte est définie en fonction de la mission. Cette modularité confère une complémentarité des capacités et des effets (observation, feux, transport, etc.) offrant souplesse d'emploi et réactivité.

L'ALAT a développé des savoir-faire qui permettent l'engagement d'unités aéromobiles à partir de tous milieux (mer, zones sommaires) et dans tous milieux (montagne, désert, zone urbaine, zone froide, de jour et de nuit). En termes de projection, 1 GAM peut se projeter de façon autonome sur 1 000 km en 24 heures. L'apport des BPC permet de projeter simultanément sur 1 500 km en 24 heures 1 GAM et 1 GTIA.

Avec ses 330 hélicoptères en service, l'engagement de l'ALAT en opérations extérieures est permanent. Actuellement, près de 300 personnels et une trentaine d'hélicoptères sont déployés au Mali (opération SERVAL), en RCA (opération SANGARIS), au Tchad (opération EPERVIER), mais aussi au Gabon et à Djibouti, pour ne citer que les détachements majeurs.

Arme de la fonction contact, l'ALAT a systématiquement réalisé plus d'un tiers des bilans lors des récentes opérations extérieures (LICORNE, PAMIR, HARMATTAN, SERVAL).

Dans ces environnements complexes, l'ALAT, c'est aussi :

- |                                  |                           |
|----------------------------------|---------------------------|
| • 25 % de missions CCA,          | • 0 suspicion de CIVCAS,  |
| • 25 % de missions d'attaque,    | • 2 personnels tués,      |
| • 25 % de tirs à moins de 100 m, | • 12 aéronefs endommagés, |
| • 0 tir fratricide,              | • 6 aéronefs détruits.    |

L'opération SERVAL (Mali) est un exemple en termes d'assimilation de l'expérience opérationnelle acquise lors des précédents engagements en Afghanistan, en Libye ou en Côte d'Ivoire. Cette opération réaffirme aussi la formation « terre » des personnels de l'ALAT.

L'opération SERVAL a valorisé l'aérocombat, conférant un ascendant déterminant aux troupes au sol, notamment par l'efficacité de l'alternance d'emploi GAM/GTIA (action autonome et combinée). Cependant, les grandes éloignations du déploiement (jusqu'à 1 200 km) ont mis en exergue la fragilité logistique et la sécurisation des FARP. Des efforts sont à faire pour la gestion I3D, la cartographie et les équipements de communication satellitaire.

Au niveau tactique, cette opération montre la nécessité de prendre en compte l'aérocombat dès la conception de la manœuvre, en recherchant la modularité et en privilégiant des actions planifiées de nuit, en intégrant les drones tactiques et en développant une chaîne renseignement dédiée aux actions d'aérocombat.

A l'issue de la conférence et lors des discussions, le colonel Turquet a notamment apporté des compléments d'information sur les points suivants :

- Apport des hélicoptères de nouvelle génération (HNG) à l'ALAT et apport des nouvelles technologies
- Attentes concernant les équipements et armements mis en place sur les hélicoptères de l'ALAT
- Perspectives opérationnelles nouvelles liées aux nouveaux matériels.



Tigre en opérations (Photo colonel Turquet)

La première de ces perspectives pour le colonel Turquet est le tir collaboratif, c'est-à-dire la capacité de traiter un objectif au-delà des vues directes, en collaboration avec un autre hélicoptère, un drone tactique, ou une unité au sol.

Le deuxième point qu'il souligne, c'est l'intégration des drones tactiques à la manœuvre des unités d'aérocombat. A titre illustratif, il s'agit de considérer le drone comme le 3<sup>ème</sup> ailier de la patrouille de Tigre et qui lui apporterait une allonge supplémentaire, une permanence sur l'objectif, plus de sûreté et des capacités complémentaires : capteurs et armement.

Enfin, l'intégration à la bulle aéroterrestre SCORPION me semble une perspective opérationnelle nouvelle. En effet, grâce à la numérisation de l'ensemble des unités d'hélicoptères, les unités d'aérocombat continueront d'être une fonction de combat essentielle au sein du futur GTIA SCORPION.



Tigre en opérations (Photo colonel Turquet)

**Thierry BON, d'après des informations données par le colonel Frédéric TURQUET**

## EMBOWXIV, Biscarosse, 5 au 26 mars 2014

Pour cette 14<sup>e</sup> édition printanière des essais OTAN EMBOW sous l'égide du SG2 (sous-groupe 2 de l'Air Capability Group 3 de la NATO Air Force Armaments Group), DGA Maîtrise de l'information était à nouveau présent sur le site de DGA Essais de missiles à Biscarosse avec ses équipes d'experts en optronique. Cet exercice s'est réalisé du 5 au 26 mars 2014 pour évaluer « grandeur nature » des tactiques de guerre optronique destinées à protéger les aéronefs contre les tirs de missiles à guidage infrarouge.



Installations au sol (Photo DGA)

La précédente campagne EMBOW XIII avait déjà eu lieu en France en septembre 2011. Pour les équipes en charge de la guerre optronique, c'est l'aboutissement d'une année de préparation pour parfaire les séquences de leurrage adaptées aux nouvelles menaces de type Manpads que cet exercice permet de mettre en œuvre. La campagne a été également l'occasion de tester en

situation réelle l'efficacité d'un matériel DIRCM britannique embarqué sur un CASA de DGA EV et la mise en œuvre d'une maquette exploratoire d'AD à imagerie représentative des menaces futures.

Pilotée techniquement par DGA Maîtrise de l'information qui représente la DGA au SG2, en partenariat avec l'EPIGE, la campagne EMBOW XIV a été une belle réussite de coopération entre les différents centres de la direction technique impliqués (DGA Essais en vol, DGA Essais de missiles et DGA Maîtrise de l'information) et les 13 autres nations participantes. Dirigé par DGA Essais en vol, avec la collaboration majeure de DGA Essais de missiles et de DGA Maîtrise de l'information et de l'armée de l'air, cet exercice a vu les aéronefs suivants mis en œuvre sur le site de Cazaux :

- C-130 Hercules belge,
- EH101 Merlin danois,
- F-18 Hornet et CH-47 Chinook espagnols,
- AB212 Bell-Agusta, CH-47 Chinook, C-130 Hercules, C-27 Spartan, EF2000 Eurofighter et GR Tornado italiens,
- F-16 norvégiens,
- F-16 et C-130 Hercules néerlandais,
- L159 Alca, JAS29 Gripen, Mi171 et Casa 295 tchèques,
- C-130 Hercules et Black Hawk suédois,
- F-18 Hornet et AS532 Cougar suisses,
- F-16 turcs,
- EC725 Caracal, EC665 Tigre, et NH90 Caïman et Mirage 2000D français.



Ces essais ont permis de tester face à un grand nombre de menaces représentatives des Manpads et des missiles air-air les nouveaux leurres Lacroix aujourd'hui dans les forces ; on peut notamment citer les leurres spectraux LIR411V1 équipant les avions de chasse français et les LIR111T6, nouveaux leurres au standard OTAN pour les hélicoptères français (Tigre, EC-725, NH90), les LIR112 leurres cinématiques pour hélicoptères ainsi que la nouvelle cartouche LIR211 bi-pain, dernière née de notre industriel de défense Lacroix. Des plateformes étrangères ont également pu tester des leurres Lacroix comme les F-16 de l'EPAF et de la Turquie, les F-18 espagnols ou les C-130 des Pays-Bas.

Beaucoup d'autres nouveaux leurres ont pu être observés, dont de nouveaux leurres spectraux et propulsés pour avion de chasse. De nouveaux enjeux se préparent déjà pour EMBOW XV qui aura lieu à nouveau en Allemagne en septembre 2015, tant dans le domaine du leurrage (multibande) que dans le domaine du DIRCM ! Rendez vous l'an prochain pour un nouveau retest !

### Rappel du principe :

Les essais EMBOW ont pour objectif d'étudier, d'expérimenter et de partager diverses techniques et tactiques de leurrage et brouillage infrarouge, cela, dans un environnement réel. Fondamentalement, EMBOW doit enrichir le niveau de connaissance mutuelle des pays de l'OTAN susceptibles de participer à des opérations communes. Pour chacun des aéronefs participant à ces essais, un rapport précisant les niveaux d'efficacité et les voies d'amélioration envisageables pour le leurrage et le brouillage est rédigé. Celui-ci vise à donner à chaque participant les moyens de



Embow XIV, nouvelle preuve éclatante d'une coopération efficace au profit des opérationnels. (Photo DGA)

dégager des pistes concrètes d'optimisation et de maîtrise de la survivabilité des plateformes aéroportées déployées en opération.

Pour évaluer les niveaux d'efficacité des différentes tactiques retenues, la plateforme doit réaliser une matrice de test (différentes présentations et distances) suivant un protocole éprouvé, notamment en respectant un nombre de répétitions adéquat. Le déroulement des essais EMBOW consiste, dans un premier temps, « à faire accrocher » différents autodirecteurs infrarouges au sol sur les aéronefs. Dans un deuxième temps, il s'agit pour les équipes de mesure et d'analyse d'évaluer le comportement

Suite page 6

## Le chapitre français La Fayette au 70<sup>ème</sup> anniversaire du Débarquement

Le Musée franco-allemand du Radar de Douvres-la-Délivrande tout près des plages du Débarquement a été le cadre des rencontres que l'Association Guerrelec, chapitre français La Fayette des Old Crows, a tenu à organiser pour marquer le 70<sup>ème</sup> anniversaire du Débarquement.

Une table ronde animée par Pierre Grandclément, président de Guerrelec, a permis de rappeler toute l'importance des contre-mesures électroniques, tant dans la préparation des opérations que dans leur déroulement. La visite du musée du radar a donné également lieu à de nombreux échanges sur ce thème.



La conférence Guerrelec de Douvres-la-Délivrande (Photo Jean-Pierre Vadet)

Ce musée a été créé à l'endroit même où était installée une importante station radar allemande du mur de l'Atlantique. Dans les blockhaus qui ont été ouverts sont rappelés ce qu'étaient ces stations radar, comment elles permettaient le guidage d'avions intercepteurs ou de l'artillerie antiaérienne ou encore quelles y étaient les conditions de vie. Des salles sont consacrées à l'Histoire du radar avec les métamorphoses qu'il a connues depuis cette



Musée Franco-Allemand du Radar (Photo Jean-Pierre Vadet)

époque ou encore au précurseur qu'avait été Christian Hülsmeier. En extérieur sont présentés des radars de la Seconde Guerre mondiale tels le « Würzburg » allemand ou le radar américain SCR 584. On y observe tout l'avantage qu'avaient pu tirer les Alliés de la maîtrise des ondes centimétriques.



Allocution du Maire de Douvres-la-Délivrande (Photo Jean-Pierre Vadet)

Une visite à ne pas manquer pour tous ceux qui tiendront à se rendre sur les plages du Débarquement pour honorer ceux qui s'y sont illustrés. Ces manifestations ont été organisées conjointement par les Associations Guerrelec (présidée par l'IGA Pierre Grandclément), l'Association des Amis du Musée Franco-Allemand du Radar (présidée par Yves Blanchard) et les Anciens de Thales (dont la Commission « patrimoine historique » est animée par Pierre Baratault, membre de Guerrelec et qui a été le vice-président d'Aicprat) et avec le soutien de la ville de Douvres-la-Délivrande qui a créé et gère ce Musée Radar.

Jean-Pierre VADET

de ces autodirecteurs accrochés sur leurs objectifs pendant que ceux-ci déclenchent des séquences de leurrage et de brouillage. Les vols sont réalisés selon un scénario préétabli simple (altitudes et vitesses stables, points de largage des leurres clairement identifiés) de manière à recueillir suffisamment d'éléments fiables pour mener des études objectives. Pour chaque passe ou « run », les équipes sol (moyens de mesure infrarouge et capteurs infrarouge) enregistrent les données et établissent un diagnostic quant au comportement du capteur infrarouge d'un missile le plus souvent de type Sol-Air à Très Courte Portée (SATCP ou MANPADS).

Les capteurs infrarouges sont instrumentés sur des tourelles toujours plus sophistiquées qui permettent de mettre les autodirecteurs de missile dans une configuration la plus proche possible d'un missile en vol en poursuite stabilisée sur la plateforme

testée. Une grande variété de capteurs (autodirecteurs) est mise en œuvre par différentes nations suivant le même protocole. Il est ainsi possible d'établir des statistiques par type de capteur. Il en est de même pour les moyens de mesure infrarouge. Processus d'étalonnage et références de sensibilité sont communs à l'ensemble des nations mettant en œuvre les moyens de mesure infrarouge (spectro-imageurs, caméras, radiomètres). Ainsi, les résultats obtenus constituent une base de données fiable et homogène pour ensuite évaluer la robustesse de la tactique en environnement de simulation numérique et estimer par exemple la distance de passage avec un missile engageant la plateforme ou encore expliquer le niveau d'efficacité des séquences testées.

Isabelle **LECUYER**  
DGA-MI

## Le 51<sup>ème</sup> AOC à Washington, deux Français honorés

La convention annuelle de l'AOC (Association of Old Crows) dont Guerrelec est le chapitre français vient de se terminer à Washington DC.

Pour la 51<sup>ème</sup> fois, l'Association of Old Crows réunissait la communauté internationale de la Guerre Electronique du 6 au 9 octobre pour sa convention annuelle afin de favoriser les échanges entre les spécialistes de ce réseau international fort de 13 500 membres en 2014. Conférences, hall d'expositions et moments conviviaux ont permis aux centaines de participants d'observer les mutations d'un réseau fêtant ses 50 ans cette année : innovation sur les composants et systèmes embarqués, évocation de concepts

opérationnels intégrant le cyberspace, description des opérations interalliées et des menaces apparues, etc.

Deux présences françaises à signaler : tout



Notre membre de Guerrelec, Olivier Terrien, reçoit son Award (Photo Olivier Terrien)

d'abord, le colonel Brun de Saint-Hippolyte a reçu des mains du président de l'AOC l'Outstanding NATO Unit Award pour son régiment. L'excellent travail accompli en Afghanistan par le 54<sup>ème</sup> Régiment de Transmissions était ainsi reconnu et distingué par les plus hautes références électroniques mondiales. Puis un membre de Guerrelec, chapitre français, Olivier Terrien, a présenté son dernier projet de sensibilisation aux présidents des chapitres nationaux de l'AOC. Destiné à susciter la réflexion d'un public non initié autour de la Guerre Electronique, son livre *Crow vs Crow* se trouve désormais dans la liste des ouvrages recommandés de l'AOC.

La prochaine convention aura lieu du 1<sup>er</sup> au 3 décembre 2015 à Washington DC, USA.

Pierre-Alain **ANTOINE**, d'après des informations transmises par Olivier **Terrien**, Membre de Guerrelec



A gauche, le colonel Brun de Saint-Hippolyte du 54<sup>ème</sup> RT reçoit son Award (Outstanding NATO Unit Award) (Photo Olivier Terrien)

## Colloque du 26 novembre au Mont-Valérien : Comment rester maître de l'Ether et du Cyberspace ?

Pour le 50<sup>ème</sup> anniversaire de l'Association internationale des Old Crows le thème **Comment rester maître de l'Ether et du Cyberspace ?** a été choisi par l'Association Guerrelec.

Destinée à enrichir la réflexion sur la problématique de l'utilisation du spectre électromagnétique, cette manifestation a pour ambition de mettre l'accent sur les principales facettes de ce sujet complexe en élargissant vers la thématique du Cyber.

Le colloque sera placé sous la présidence de Madame Patricia ADAM, députée du Finistère, Présidente de la commission de la défense nationale et des forces armées, et de Monsieur Jean-Marie BOCKEL, sénateur du Haut-Rhin.

La journée sera organisée autour de trois tables rondes qui réuniront chacune, autour d'un modérateur, trois intervenants dont l'expérience, la connaissance et la pensée sont les gages de la qualité et de la réussite de ce colloque. Seront successivement abordés les thèmes suivants :

- « **Les enjeux de la maîtrise du spectre** »,
- « **Les outils et technologies actuels et en préparation** »,
- « **Les politiques industrielles face à ces menaces** ».

Au cours de ce Colloque un hommage sera rendu à Monsieur Jean TURCK, 103 ans, pionnier de la Guerre Electronique française.

Pierre-Alain **ANTOINE**

# Les derniers potins GE de l'été.

« Il » fit sa dernière apparition opérationnelle au cours de l'été 2014 lors de manœuvres franco-saoudiennes sur la BA 133 de Nancy-Ochey.

Le thème de cette manœuvre dans laquelle la Royal Saudi Air Force avait déployé 6 F-15C/D et un KC-3B de ravitaillement en vol (ce dernier était stationné sur l'aérodrome de Metz-Nancy-Lorraine). Quant à l'armée de l'air, elle avait mis en œuvre des Mirage 2000 C/RDI, des Mirage 2000 D, des Mirage 2000-5F, des Rafale, des Alphajet et des EC-725 « Caracal ». Ce thème donc était l'« Air Interdiction » et RESCO/CSAR.



F-15C saoudien à Nancy-Ochey (Photo Pierre-Alain Antoine)

« Il », c'était un système SA-8 « Gecko » que j'étais allé chercher personnellement en 1993, dans un dépôt ex-NVA (l'armée de l'ex-Allemagne de l'Est) situé dans une forêt au nord de Dresde, après la réunification de l'Allemagne alors que j'étais le directeur du Polygone de Guerre Electronique à Ramstein.

Quelques semaines plus tard, j'assistai, très ému, à la dissolution de l'Escadron de Guerre Electronique (EGE) qui regroupaient les trois sites du Polygone en France (ancienne base aérienne canadienne de Grostenquin en Moselle, ancienne base américaine de Chennevières, à l'est de Lunéville en Meurthe-et-Moselle et l'ancien fort des Adelphe, ancien fort Séré des Rivières de la ceinture des forts de la ville d'Epinal, chef-lieu des Vosges). Ainsi, la France, qui avait signé un MOU (Memorandum of Understanding) en 1979 avec les Etats-Unis et l'Allemagne afin de mettre en œuvre cette unité tri-nationale, fermait cette unité sous prétexte d'obsolescence. Alors que nous assistions à la dernière mission à Epinal entre le T-13 (simulateur SA-6 « Gainful ») et des Mirage 2000 D de la 3<sup>ème</sup> escadre de Nancy-Ochey, les USA proposaient de nous racheter ce T-13 (trois seulement ont été construits dont le T-13 français qui était le plus moderne des trois). Alors ce T-13 était-il si obsolète que cela ... ?

Nous avons appris quelques semaines plus tard qu'un Boeing 777 de la compagnie Malaysian Airlines avait été abattu par deux missiles SA-15 (méthode russe de toujours tirer deux missiles sol-air à la fois)...



Le premier RC-135 de la RAF arrive fin 2013 à Waddington (Photo Pierre-Alain Antoine)

Une autre réflexion : le DC-8 « Sarigue » NG a été retiré du service seulement deux ans après sa mise en service, il y a quelques années déjà et nos deux C-160G « Gabriel », bien que récemment modernisés, ont bien du mal à remplir la mission SIGINT tout simplement parce que les performances de deux avions sont différentes (l'un était stratégique et l'autre, tactique).

M'entretenant récemment avec un ancien ministre de la Défense, j'ai eu l'occasion de lui rappeler qu'en matière de renseignement : « on ne donne pas un renseignement, on l'échange ; si l'on a rien à échanger, on n'existe pas » et de lui demander comment on gérait la crise en Ukraine et en Crimée sans un avion SIGINT stratégique alors que la Royal Air Force vient de mettre en service le premier de ses trois RC-135 commandés à la société L3. Ce ministre m'a avoué qu'à l'époque nous aurions pu faire mieux.

Est-il trop tard ou avons-nous les moyens de rattraper cela ?



SA-8 du PGE à Nancy-Ochey (Photo Pierre-Alain Antoine)

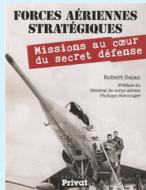


Les deux Sarigue réunis pour la première et la dernière fois le 25 juillet 2001 au Bourget (Photo © SIRPA Air)

Pierre-Alain ANTOINE,  
ancien directeur du Polygone de GE (1992-95)



## FORCES AÉRIENNES STRATÉGIQUES, MISSION AU CŒUR DU SECRET DÉFENSE



**Auteur : Robert Galan**  
**Editeur : Edition Privat**  
**ISBN : 978-2-7089-9255-9**  
**Pages : 220**  
**Prix : 18 Euros**

Nées de la volonté du Général de Gaulle qui voulait affranchir la politique de défense française d'une tutelle internationale et faire de la France une nation de tout premier plan, les FAS ont été créées en 1964. Dans cet ouvrage, Robert Galan, ancien pilote des FAS, nous plonge dans le cœur du « secret défense » et d'un demi-siècle d'opérations au service de la paix. Des récits épiques, poignants - parfois teintés d'ironie - où se distingue le sens aigu du courage, du devoir et de la camaraderie qui unit les « aviateurs du nucléaire » aux mécaniciens d'exception en un seul corps.

A lire pour entrer dans l'ambiance de la période du Mirage IVA.

## MA VIE DANS LES SERVICES SECRETS, 1943-1945



**Auteur : Noreen Riols**  
**Editeur : Calmann-Lévy**  
**ISBN : 978-2-7021-5526-4**  
**Pages : 340**  
**Prix : 19,50 Euros**

Lorsque la France s'effondre en 1940, Winston Churchill aide de Gaulle à passer à Londres et fonde le SOE ou Special Operations Executive. Les buts de cette armée secrète sont d'infliger le maximum de pertes aux Allemands, créer des réseaux de résistance et d'informer Londres des mouvements de

l'ennemi. Pour cela, il faut former des agents bilingues capables de sauter en parachute, de tuer par tous les moyens, d'envoyer des messages radio, etc... et, tout cela, dans le plus grand secret.

C'est ainsi qu'après avoir travaillé dans une usine de munitions, Noreen Riols à peine sortie de l'adolescence est convoquée à Baker Street, siège du SOE... Soixante-ans plus tard, survivante de la section F (comme France) avec Bob Maloubier, Noreen se souvient...

Tour à tour aimables, plaisants, humoristiques et terrifiants, ces souvenirs sont l'œuvre d'une femme aussi exceptionnelle qu'extraordinairement modeste. Aujourd'hui, Noreen Riols qui vit en famille dans les Yvelines est l'un des derniers témoins en France du SOE.



## UN MÉCANO DE L'ARMÉE DE L'AIR PARMI TANT D'AUTRES, MÉMOIRES D'UN MÉCANICIEN DE L'ARMÉE DE L'AIR



**Auteurs : Christian Borel**  
**Editeur : Edilivre**  
**ISBN : 978-2-332-74348-0**  
**Pages : 190**  
**Prix : 16,50 Euros**

L'auteur, ancien mécanicien avion dans l'armée de l'air, a servi dans la chasse, dans les hélicoptères et dans les avions de transport, en métropole come en outremer. Il a été membre des « équipages de Nord Gabriel » qui ont emprunté les couloirs de Berlin, mais aussi dans les missions spéciales au Tchad. Un important cahier iconographique illustre l'ouvrage.

A glisser dans sa bibliothèque.

## LA GUERRE DU VIETNAM



**Auteur : John Prados**  
**Editeur : Perrin**  
**ISBN : 978-2-286-08138-6**  
**Pages : 835**  
**Prix : 30,50 Euros**

De la fin de la Seconde Guerre mondiale jusqu'à la chute de Saïgon en 1975, John Prados livre le seul récit complet et la première analyse globale de la guerre du Vietnam. S'appuyant sur des documents récemment déclassifiés et un large éventail de sources vietnamiennes et internationales, l'auteur peint une fresque magistrale où idéologies et armées s'entrechoquent. Tour à tour, récit enlevé, essai novateur et témoignage personnel émouvant, cette œuvre monumentale dresse le bilan définitif d'une guerre nouvelle (surtout dans la GE), qui bouleversa les Etats-Unis et modifia l'équilibre planétaire.

Ouvrage de référence.

## CROW VS CROW



**Auteur : Olivier Terrien**  
**Editeur : Oty Productions**  
**ISBN : 978-2954199672**  
**Prix papier : 10,00 Euros**  
**Prix eBook : 6,99 Euros**

A l'occasion des 50 ans de l'Association of Old Crows dont Guerrelec est le chapitre français, Olivier Terrien publie une déclinaison illustrée de ses 36 Stratagèmes de la Guerre Electronique. Une approche originale et ludique pour ouvrir notre domaine technique à un large public grâce à la force de l'image et des textes dynamiques.

Deux corbeaux ou « crows » en anglais s'affrontent à chaque nouvelle double page et reproduisent l'affrontement entre glaive et bouclier qui se déroule aujourd'hui sur le spectre électromagnétique.

Préfacé par le président de l'AOC, ce livre illustré fera date dans la bibliothèque de la GE puisque l'AOC l'a placé dans ses « livres recommandés ».

## ESSAI NUCLÉAIRE - LA FORCE DE FRAPPE FRANÇAISE AU XXI<sup>È</sup> SIÈCLE : DÉFIS, AMBITIONS, STRATÉGIE



**Auteur : Philippe Wodka-Gallien**  
**Editeur : Lavauzelle**  
**ISBN : 978-2-7025-1606-5**  
**Pages : 226 dont 10 pages photos couleurs**  
**Prix : 23,60 Euros**

Arrivant fort à propos, ce dossier de Philippe Wodka-Gallien revient en détail sur tous les fondements de notre dissuasion, à travers ses aspects stratégique, politique, budgétaire, technologique et opérationnel, voire culturel.

Le message central tient en une phrase : consolidant un tissu industriel stratégique porteur d'emplois très qualifiés (civils comme militaires), la dissuasion projette notre concept de défense loin dans l'avenir, au regard d'un monde instable qui renoue avec les logiques de puissance et de course aux armements. « On retrouvera avec plaisir, dit Philippe Wodka-Gallien, le témoignage de Pierre-Alain Antoine, sur les origines du Polygone de Guerre Electronique et ses missions en Mirage IV ».

Fidèle à Guerrelec, l'auteur souligne les multiples apports de la GE et de l'électronique à la crédibilité de la force de frappe, et, in fine, à l'efficacité des forces conventionnelles. Il s'agit bien là d'un travail de conviction qui montre en quoi le nucléaire, à travers ses multiples dualités, peut être l'instrument de relance de notre économie.



## Les sociétés membres de Guerrelec

- AMESYS • ARINC • DCI AIRCO • EADS ASTRIUM + CASSIDIAN • INEO DEFENSE • LACROIX • MBDA • RAFAUT
- THALES Communications & Security • THALES Systèmes Aéroportés • THALES Université • VECYSYS

Association Guerrelec AOC French La Fayette Chapter. Directeur de la publication : Pierre Grandclément, Rédacteur en chef : Pierre-Alain Antoine.

Réalisation et impression : GT PRINT : 01 34 52 18 88

Ont collaboré à cette édition : Pierre-Alain Antoine, Pierre Baratault, Thierry Bon, Fabrice Cinquetti, Pierre Grandclément, Isabelle Lecuyer, Olivier Terrien, Jean-Pierre Vadet.